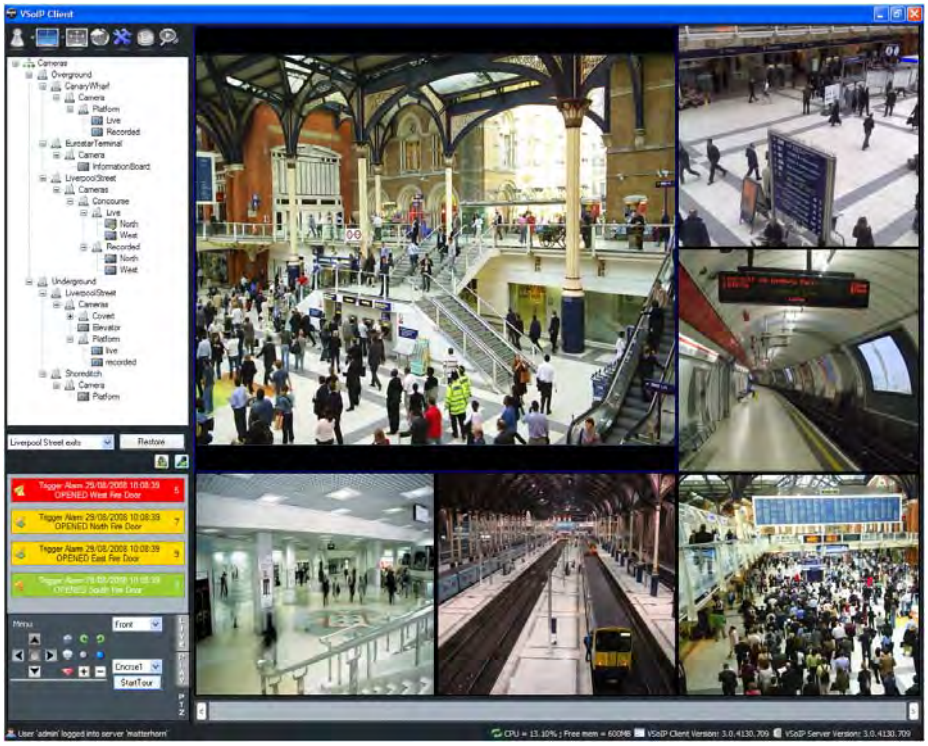
MANAGEMENT SOFTWARE

VSOIP PRO 3.1

USER MANUAL



17 May 2011 ZNS-CSC

Table of Contents

1 System Overview 7

Overview 7
System Components 7
Surveillance Suite Architecture 8
IP Camera and DVR Configuration 8
System Environment 8
Network Traffic 8
Infrastructure 8
Configuring Stream Settings 9
System Hardware Considerations 10
System Software 10
System Licensing 11
Licensing Overview 11
VSoIP Licensing 12

2 The Server Component 13

VSoIP Pro Server Overview 13
Server Prerequisites 14
Hardware Specification 14
Operating System 14
Additional Mandatory Software 15
Optional Software 15
Before Installing the VSoIP Pro Server 15
All Operating System Settings 15
Networking Settings 15
Firewalls and Port Usage 16
Switching off Power Saving 17
Installing the VSoIP Pro Server 17
Installing the the VSoIP Pro Client on the Same Computer 18
Offline Licensing 18
Using the VSoIP Pro Server 19
Starting the Server Manually 19
Starting the Server Automatically 20
Stopping the Server 20
Troubleshooting 20
How can I be sure the Server is running? 20
Network Time Server 21

3 Installing the VSoIP Pro Client 22

VSoIP Pro Client Overview 22
Prerequisites 23
Hardware Specification 23
Operating System 24
Additional Mandatory Software 24
System 24
Before Installing the VSoIP Pro Client 24
Operating System Settings 24

Networking Settings 25
Firewalls and Port Usage 25
Adding Trusted Sites 26
Additional Security Software 27
Direct-3D Hardware Support and Microsoft Direct-X 9.0c or above 27
Installing the VSoIP Pro Client 28
Offline Licensing 29
Post-installation Checklist 29
Network Time Server 29
Starting and Stopping the Client 29

4 Client Configuration 30
System Overview 30
Getting Started 30
User Configuration 31
Adding a New User 32
Changing User Passwords 33
Temporarily Preventing a User from using a Server 34
Deleting an Existing User 35
Logging in as a Different User 35
User Group Configuration 36
Creating a User Group 36
Copying a User Group 37
Deleting a User Group 37
Device Configuration 38
Adding Devices 38
Configuring Devices using the Web Interface 43
Deleting Devices 44
Configuring Video Sources 45
Configuring Triggers 46
Configuring Pan-Tilt-Zoom Capabilities 47
Configuring Audio 48
Communicating Using Audio 49
Configuring Sequences 50
Configuring PTZ Keyboard Support 51

5 Using VSoIP Pro to Monitor your Site 52
Working with Live Video and PTZ 52
Multi-head Monitor Support 53
Specifying Video Pane Layout 54
Starting and Stopping Live Video 55
Using Digital Zoom 56
Taking a Snapshot of Live Video 56
Control of Pan-Tilt-Zoom 57
Viewing Sequences 59
Stored Views 60
Updating a Stored View 60
Deleting Stored Views 61
Recovering a Previously Stored View 61
Working with Alarms 62
Overview of Alarm Display 62
Viewing Properties of an Alarm 63
Acknowledging an Alarm 63

Closing an Alarm 64
Playing Back Recorded Video....65
Discovering Recorded Footage 65
Playing Back Recorded Footage 67
Using Digital Zoom 68
Taking a Snapshot of Recorded Video 69
Synchronising Playback of Recorded Footage....70
Exporting Recorded Video 70
Exporting One or More Recordings 70
VSoIP Player....71
Audit Trail Configuration....72
Audit Trail Profiles....73
Audit Trail Management....74

6 Complex Alarm Configuration 75
Simple, Scheduled and Device-specific Alarms....75
Simple Alarms....75
Scheduled Alarms....75
Device-Specific Alarms....75
Complex Alarm Actions....76
Displaying Live Video on all Connected Clients and Video-walls 76
Auto-Acknowledging Alarms....77
Activating a Relay on an Alarm....78
Understanding Alarm Processing....78
Creating Complex Alarms 79
Copying a Complex Alarm 84
Enabling/disabling a Complex Alarm 84
Using the NOT Boolean Operator 84
How Complex Alarms Work 85
Example of Complex Alarm Processing....86

7 Accessing VSoIP Pro Remotely using a Web Browser 88
Overview of Remote Access....88
Prerequisites 88
Using Remote Access....89

8 Configuring PTZ Keyboards with VSoIP Pro....91
Overview 91
Prerequisites 91
Installing the Hardware Keyboard Driver 91
The Software Keyboard Driver....91
Starting and Stopping the Software Keyboard Driver 92
Configuring the Software Keyboard Driver 92
Assigning Keyboard IDs....93
Using the Keyboard to View Video....95

9 Using PTZ Keyboards with VSoIP Pro 96
Getting Started 96
Identifying Devices and Video Panes....96
Using a PTZ Keyboard....96
Troubleshooting PTZ Keyboards 97

10 Designing Mapsets 98
Mapsets Overview 98
Designing Mapsets 99
Creating a Mapset without a Map Design Tool 99
Typical Workflow 99
Placeholder Map Page 101
Page Links - Textual 102
Camera Links - Graphical 102
Alarm Links 104

11 Configuring and Using Mapsets 107
Introduction 107
Adding Mapsets to the Server 107
Associating Map-links with Devices 108
Deleting Mapsets 108
Troubleshooting 109
Using Mapsets 109

12 System Administration 111
Restoring Factory Defaults 111
Reusing Devices, Users and Groups 112
Exporting Devices, Users and Groups 112
Importing Devices, Users and User Groups 113
Viewing System Information 114
Default Settings 115
Alarm Viewing 116
Changing Client Settings 117

13 NVR Component 119
NVR Overview 119
Prerequisites 120
Before Installing the NVR 121
All Operating System Settings 121
Networking Settings 121
Firewalls and Port Usage 122
Installing the NVR 123
Using the NVR on the Same PC as the VSoIP Pro Server 123
Installing the NVR on a Separate PC 123
Offline Licensing 124
Upgrading the NVR 124
Starting the NVR 124
Starting the NVR Manually 125
Starting the NVR Automatically 125
Stopping the NVR 125
Troubleshooting 126
Expected Performance 126
Network Time Server 127

14 NVR Configuration 128
What is a Recording Job? 128
Types of Recording Job 128
What Happens When a Partition Becomes Full? 130
Creating a Recording Job 130

Editing Recording jobs....131
Disabling/Deleting Recording jobs....132
NVR Failover....132
Using Stream Sampling to Reduce Required Storage Space....133
Using the VSoIP NVR to Broadcast a Video Source....134
Alarm-Based Recording — Pre- and Post-Alarm Buffers....135

15 Using the VSoIP Gateway....136
Overview....136
Configuring the VSoIP Gateway Service....136
Adding a Device....138
Creating Sessions....139
Displaying Video....140
Displaying Video in a Web Browser....140
Displaying Video using the VSoIP Export Player....140
Displaying Video using VSoIP Pro or VSoIP Video-wall....141

Appendix A – Maintenance Information....143
Opening a Command Prompt in Microsoft Windows....143
Opening the Run dialog....143
Finding out the IP Address of Your Computer....143
Determining PC Port Usage....144
Windows Events – Using the Event Viewer....145
Displaying Hidden or System Files....145
Configuring Application Log to Overwrite Oldest Entries....147
Viewing Windows Services List....148
Checking Connectivity of a Networked Device or Computer....149
Troubleshooting....150
Providing Technical Support Information....151
Specifying the Logging Level....153

Appendix B – Supported Devices....154
Additional Device Support....156
Supported Keyboards....156

Appendix C – Specific Device Considerations....157
Adding ZV-S306 and ZN-D2024 Devices to VSoIP Pro....157
Adding DRH-DVD and DR4H Lite DVRs....157
Adding Generic ONVIF Devices....158

Appendix D – NVR Partitions and Partition Groups....159
Partition Overview....159
Partition Modes....159
Partition Groups....160
Choosing a Recording Partition....161
....162

Index....163

Chapter 1 – System Overview

This chapter contains information on the following:

- Overview
- System Components
- System Environment
- System Licensing

Overview

The VSoIP Pro surveillance suite provides a mechanism primarily for viewing, recording and reviewing video via computer network hardware, networked cameras, networked digital video recorders (DVRs), networked computers, systems software and bespoke software.

This system is a complex one with Ganz and other manufacturers supplying differing hardware with different feature sets and characteristics. In such systems the adherence to standards is the route relied on to make the overall system work.

The system architecture is based on an Internet Protocol (IP) network — all communication is performed over IP networks — and the surveillance suite software relies on Microsoft Windows technologies.

System Components

Table 1 System Components

Client	A client is a software entity that presents a view of the current state of the surveillance suite. It makes requests to a server which permits certain actions to be carried out by the client. The client can also act in an administrative capacity allowing the configuration and maintenance of the whole system.
Server	The server is a software entity that acts as a central decision and control centre for the whole system. It provides a series of services to clients. It ensures that actions made by the clients, if appropriate, update the surveillance system. The server installation procedure includes the VSoIP Server, VSoIP NVR and VSoIP Gateway.
Networked Video Recorder	The NVR is a software entity that stores network streams originating from IP cameras and networked digital video recorders onto a storage device and retrieves these at a later time. The “recorded” stream is not tampered with in any manner so the evidential integrity of recorded video is maintained. The NVR is installed automatically as part of the server installation process, however it must be licensed before use. For more information, see “NVR Overview” on page 119.
Video-wall	The Video-wall is a software entity that displays video originating from IP cameras and networked digital video recorders in a matrix style layout.
Transcoder/broadcaster (Gateway)	A combined transcoder/broadcaster software entity converts media streams originating from network streams from IP cameras and networked digital video recorders, from folders of image files and from video files and broadcasts media streams transcoded to alternative encoding, framerate, resolution and bit-rates. These transcoded and broadcasted streams are later consumed by clients, Video-walls or Networked Video Recorders. The VSoIP Gateway is installed automatically as part of the server (or NVR) installation process. It does not require licensing.

Caution: The incorrect shutdown of the recorder could risk loss of previously recorded footage, or recorder system failure. See “Stopping the NVR” on page 125 for more information.

Surveillance Suite Architecture

When the system components are installed on computer hardware and interconnected via a computer network, and given access to compatible IP cameras and networked digital video recorders, the components act together to form a surveillance system.

Typically the surveillance system will consist of:

- At least one networked video source, either camera or recorder (but ordinarily many more).
- A single server component (comprising device server, NVR, and stream server).
- At least one client (but usually several).
- Video-wall, NVR, and transcoder/broadcaster components are optional. There can be several NVR and Video-wall components within the system.

Note: There is only one server component within the surveillance system. There can be several surveillance systems on the same network but note that each system has a single server component at its core.

IP Camera and DVR Configuration

A list of compatible devices is supplied separately in Appendix B, "Supported Devices". Please note that devices should be configured in the manner indicated in the list at system installation time. Device configuration support is not provided by the surveillance software suite.

System Environment

The system makes use of Internet Protocol based computer networks. The construction of such networks is beyond the scope of this document however the network design must take into full consideration the large quantity of data transferred across networks by surveillance systems.

It is useful however to have a high level discussion of the major areas that should be addressed when designing such a network and choosing the communication parameters of the IP cameras and networked digital video recorders attached to the network.

Network Traffic

Video streamed from IP cameras and networked digital video recorders is the major configurable source of traffic on the network. The quantity of data traffic from each source accumulates as it is consumed by increasing numbers of devices.

Furthermore, since NVRs replay recorded network streams, the amount of data traffic generated is the same as that of the original recorded stream. Multiple playback sessions of the same recorded stream result in an accumulation of data traffic in line with the number of playback sessions. A transcoder/broadcaster software component also adds to network load since it must consume media streams for analysis.

It is therefore critical that IP cameras and networked digital video recorders are configured with a view to the number of potential viewing clients, Video-walls and NVRs recording them. Where there is a requirement for remote sites to view media streams over a restricted bandwidth connection, a transcoder/broadcaster software component can be used to present suitable bandwidth streams.

Infrastructure

When planning system infrastructure, you should take the following into account:

- Cable connections to a typical network switch device have maximum rates of 100 or 1000 megabits per second.
- Network connection between a device and a network switch can be:

    - Half-duplex – they can either send or receive traffic at any given moment.
    - Full-duplex – they can send and receive traffic at the same time.
- A network connection might have traffic from:
    - A single IP camera. or networked digital video recorder (DVR) only.
    - Many IP cameras and networked DVRs (in the case of Video-walls).
    - IP cameras, networked DVRs and played-back network streams (in the case of NVRs).
    - A transcoder/broadcaster. This software component receives media streams and generates them.
- There may be non-surveillance network data on the same network.
- Multicast traffic may help reduce bandwidth requirements. However, it may not be supported by the surveillance suite components.
- A network time sever. The presence of a hardware or software based time server is a mandatory requirement. All IP cameras, encoders, networked digital video recorders, server and client computers should obtain their base time from the network time server. For evidential purposes, the central time server should synchronise itself with an external real-world time source. Where there are multiple surveillance site locations, local time servers in each location should provide time to the site. Each local time server should coordinate with the same external real-world time source.
- Storage systems for recordings should be very high speed, large capacity integrated or external Direct Attached Storage (DAS) or Storage Area Networks (SAN). On no account should Network Attached Storage (NAS) be used. Also, when configuring external DAS or SAN systems, the network delivering the video streams from the CCTV network should not be the same network used to attach the storage.

Configuring Stream Settings

When configuring IP camera and Networked DVR stream settings, you should consider the following:

- Generally more traffic is generated by:
    - High resolutions.
    - High bitrates.
    - High frame-rates.
    - High frame-rate MJPEG streams, which generally tend to generate more traffic than high frame-rate MPEG4 or H.264 streams of the same resolution.
- More traffic is generated by MJPEG by high frame quality / low compression factor.
- More traffic is generated by MPEG4 or H.264 by:
    - High I-frame quality.
    - Excessively high P-frame quality.
    - Low P-frame frequency/high I-frame frequency.
    - Type of scene observed by camera(s): e.g. more data traffic is generated by: PTZ cameras that move through tours of presets, or are frequently moved; noisy feeds from analogue cameras; night-time viewing and automatic gain causing noise, scene subject to motion – crowd scenes, busy roads, in-vehicle safety cameras, etc.
- Using H.264/AVC (MPEG4-part10) encoded video network streams can achieve equivalent video quality to MPEG4-part2 encoded video network streams at lower bandwidth. Consider using H.264 encoding for more efficient use of bandwidth particularly when using mega-pixel video sources.

    Note: H.264 can require more CPU power to decode than the equivalent stream encoded in MPEG4. Please consider this when interpreting PC specification requirements.
- Careful infrastructure planning will lead to an overall surveillance system that can be relied on. It is important to consider any network links that are heavily loaded by data traffic — typically these will be links to NVRs and Video-walls.

- It is also worth noting that when viewing live video from IP cameras and networked DVRs on a switched network, data is normally routed directly from the IP camera or networked DVR to the software viewing that camera or networked DVR, i.e. it is not received by the server component and then forwarded on to the viewing clients.
- Some IP cameras allow for different streaming rates, depending on which encoder within the camera is connected. One use of such a facility is to have one encoder on the IP camera set to typical live view settings and another encoder in the same camera set to typical recorder settings.
- Mega-pixel cameras require considerable care when deployed within a surveillance system. They can generate considerable traffic, due to their high resolution when used at 25 or 30 frames per second and when using MJPEG. The client software component will consume more PC resources than with a CIF/SIF resolution stream and thus either the specification of the PC should be revised in light of the higher decode and rendering requirements, or the number of concurrently displayed streams should be reduced, or both. If NVRs are used to record high-definition, mega-pixel network streams, these put a large load on the recorder, consuming a larger percentage of the available network connection bandwidth and consuming more storage space per second than CIF and 4CIF resolution streams.
- Predicting network traffic can be difficult so it is highly recommended that a safety margin be built in to accommodate sudden bursts of higher than average data traffic caused by a faulty camera, or similar.
- The network's ability to support multicast is important — the discovery system used in the surveillance suite is based on multicast and broadcasting. If multicast support is impossible, computers running the client software component can still locate the server component if the server's IP address is known.

  Note: Multicasting is used by VSoIP Pro for server discovery and for streaming media. For this to work, a network that suports IGMP version 2 is required. Network switches should be set to IGMP snooping and where routers are used these should be set up to permit multicasting.

System Hardware Considerations

When considering optimal hardware for the surveillance system, you should consider that:

- The server and NVR software components have a serving behaviour and as such will benefit from computer hardware optimised for the role of serving.
- The client (and optional Video-wall) components have graphical display behaviour, and so benefit from computer hardware optimised for multi-media graphical display. It may be useful to add specialist display adapters that provide dual- or quad-head capability. Such display adapters must have the functional ability to perform Direct-3D rendering in hardware, i.e. not offload this work to the computer system's host processor.

System Software

The surveillance suite components are designed to run under the recommended operating system. It is assumed that the operating system installed on computer hardware is that as installed by the computer manufacturer or installed from a genuine copy of the Windows installation media.

Caution: Anti-virus, anti-spyware and software firewall products should not be installed on surveillance computers.

No additional software other than that described as prerequisites for the various surveillance system components should be installed. Adding additional software could have unforeseen impact on the satisfactory performance of the system.

It is common for IT personnel to make changes to various aspects of Microsoft Windows such as locking down certain features or applying various operating system group policies. These types of changes are not supported by the surveillance software components.

Microsoft's in-built automatic update feature should be disabled. Instead, updates to the operating system should be carried out prior to installing the surveillance software, and then during planned system maintenance. If automatic updating is enabled unexpected behaviour such as setting changes and unplanned system restarts might occur.

It is important to update all operating system device drivers, particularly for network adapters (and graphic adapters for clients and Video-wall components); it is best to use the latest drivers available from the computer manufacturer. If you find that the computer manufacturer uses hardware from a third party, please be certain that using the third-party's driver is appropriate — often computer manufacturers obtain specially crafted variants of the third party's hardware making the usual driver from the third party less than optimal, or completely incorrect.

All surveillance suite software components use Microsoft's .Net framework. This must be installed on all computers. The setup program for the surveillance software will attempt to install the appropriate version of the .Net framework from Microsoft's web-servers if it is not detected on the computer.

The client surveillance suite components use Microsoft's Direct-X. This must be installed prior to running the client software, and can be obtained directly from Microsoft.

Server and NVR software components use Microsoft's SQL Express 2005 database management system. This must be installed on all computers using these components. The setup program for the server and NVR surveillance software components will attempt to install the appropriate version of the SQL Server 2005 Express if it is not detected on the computer.

Caution: It is recommended that the SQL Express 2005 database management system uses its default values. It should not be secured in a way that prevents the server or NVR from creating or accessing databases. SQL Express should only manage those databases added by the server and NVR software.

System Licensing

Licensing Overview

Some surveillance system software components require a license key to operate.

A license key is supplied for each software component purchased that requires one. To license a component, the key must be entered when requested, or the appropriate licensing application for the software component must be executed.

On entering the license key, the software component contacts a licensing server over the Internet. The software component collects identifying features of the computer executing the component, encrypts this information along with the license key and sends this to the licensing server. The licensing server decrypts this information and if the license key is unused, it associates the identity with the key and sends an encrypted license to the computer licensing the software component.

The identifying features of the computer used include:

- The IDs of the processor(s).
- The serial number of the hard drive(s).
- The machine (MAC) address(es) of the network card(s).

There is a level of tolerance in the licensing system which allows some of the identifying features of the hardware to be changed, e.g. the hard-drive could be changed without causing a license validation failure. However if too many distinguishing elements have changed then the validation of the license will fail. It will then be necessary to obtain a new key from your software vendor. Your software vendor may charge you a fee to obtain a replacement license key, or you may have to purchase a new one.

Note: Some computers do not have sufficient devices to accommodate a tolerance. In such cases, changing a component within the computer will require a new license key.

If the license file for a software component is deleted from the computer then the original key for the software component can be used to relicense the software component *on the same computer*. The original license file will be recreated.

Caution: Licensed software components do not need access to the Internet. It is only during licensing that an internet connection is required. Normal day-to-day running of a licensed software component does not require internet access.

VSoIP Licensing

The VSoIP Pro 3.1 Management Software Suite consists of two main components: the client and the server. Both are Microsoft .net based products for Microsoft Windows operating systems.

- The VSoIP Pro Client application is designed to allow an end user to view live video and play back recorded video, as well as monitoring alarms originating from sources such as cameras, encoders, networked DVRs and VSoIP Pro NVRs. The VSoIP Pro Client requires a license, which is provided when shipped.
- The VSoIP Pro Server runs in the background as a system service, controlling access to surveillance resources and providing a number of capabilities whether or not a user is logged in. The server contains various elements, including :
  - VSoIP Pro Server - handles administration and resource management. The server is licensed by default during the installation process.
  - VSoIP Pro NVR - handles recording and playback of video sources. This is installed during installation, but requires a license key to become operational:
    - If installed on the SAME PC as the VSoIP Server, the VSoIP Licensing Helper must be used after installation is complete to license the VSoIP NVR.
    - If installed on a DIFFERENT PC from the VSoIP Server, a unique NVR license key should be used during the installation process. This effectively disables the server element and enables the NVR.
  - VSoIP Pro Gateway - Allows re-coding of video streams for transmission over varying network types. This is installed and licensed by default during server installation.

Chapter 2 – The Server Component

This chapter contains information on the following:

- VSoIP Pro Server Overview
- Server Prerequisites
- Before Installing the VSoIP Pro Server
- Installing the VSoIP Pro Server
- Using the VSoIP Pro Server
- Troubleshooting
- Network Time Server

VSoIP Pro Server Overview

The VSoIP Pro Server software component (the “server”) is a Microsoft .Net framework based service for Microsoft Windows operating systems. It runs a series of background tasks irrespective of whether an operating system user is logged in or not. The server provides several services: device management, alarm management, user management, authentication, HTML map serving, recording, remote control interface and transcoding.

Note: The VSoIP NVR is installed by default during the server installation process. However, to make use of its recording capabilities, you must first license the NVR. For more information, please see Chapter 13, "NVR Component".

The server is designed to control access by computers executing the client software component (the “client”) to surveillance resources such as IP cameras, networked digital video recorders (DVRs), computers executing an NVR software component (the “NVR”) and computers executing a Video-wall software component (the “Video-wall”).

- The server monitors events on various IP cameras, DVRs and NVRs, raising alarms on those clients permitted to receive events.
- The server is responsible for maintaining an audit trail. The audit trail is stored in a Microsoft SQL Express 2005 database either on the same computer as the server or on another networked computer.
- The server also coordinates access to the NVRs within the system.

Initial configuration and day-to-day operational control of the surveillance system is via clients connected to the server. Clients discover servers on the network using a multicast based discovery broadcast. Clients on networks that do not have broadcasting ability must use the IP address of the computer on which the server is executing. Communication between clients, servers, Video-walls and NVRs is via .Net remoting. Communication between clients and Video-walls is via HTTP.

The server runs using a local system account, either LocalService or NetworkService. These accounts are built-in accounts in Microsoft Windows and do not need to be created.

The computer used to run the server should not be considered to be a general purpose PC and should not be used for other tasks that might starve the server of system resources.

Note: It is possible to run a client and/or an NVR on the same computer as the server but this can lead to a conflict of resources and as such is discouraged in all but the smallest of systems.

Server Prerequisites

This section details the minimum hardware, operating system and software required to run the VSoIP Pro Server.

Note: On large scale enterprise installations, PC specifications should be independently assessed for number of cameras, amount of storage and number of clients. Local conditions should also be taken into consideration.

Hardware Specification

The following is the minimum hardware specification required to provide full frame rate video for 25 streams, without dropped frames, video corruption or latency, for 1 Mbps, 25fps, CIF resolution MPEG4 encoded PAL video with one I-frame every 10 seconds.

Caution: It is highly recommended that you consider the different demands of the bit-rates, resolutions, frame rates, levels of compression and codec types of the system you are implementing when compared with this specification to ensure that your own system has the system performance that matches the demands it is likely to make. In addition, it is wise to add a safety overhead in addition to this to accommodate operating system efficiency changes over time.

- Server or workstation, architecture 32- or 64-bit.
- CPU 2.4 GHz, or greater - e.g. Intel® Core™ 2 Quad Q6600 Quad Core Processor.
- Memory: 4096MB.
- Hard Drive/Storage - 500GB SATA Hard Drive (or other very high performance drive).
- Optical Drive — DVDROM (for installation).
- 100 Base-T network card configured for full duplex.
- Uninterruptable Power Supply (UPS) system.

  To prevent system corruption due to power loss, a UPS system must be installed. This should be of a type that shuts down the operating system automatically if the utility power does not resume before the UPS power fails.

  To prepare for this possibility, the computer's power-on settings, operating system, and the UPS system should be configured so that the computer is powered on and the operating system is automatically rebooted as soon as utility power is restored.

Operating System

The recommended operating system is Windows 7 (Pro Edition). The minimum requirement is Windows XP Professional – service pack 3, or Windows Server 2003 Standard Edition – service pack 2.

Note: The VSoIP Pro Server has been tested and verified on Windows 7 32-bit systems. Installation **must** be carried out as Administrator. To run the program, you must right-click VSoIP Pro Server in the Start menu and select "Run as Administrator".

The VSoIP Pro Server is compatible with Windows 7 64-bit systems.

Note: Certain ports must be opened for VSoIP Pro to operate correctly. For more details see “Firewalls and Port Usage” on page 16.

Caution: In geographical regions where different calendar types are used, please ensure that your regional Date/Time setting is set to use the Gregorian calendar.

Additional Mandatory Software

- Windows Installer 3.1.
- Microsoft .Net Framework 3.5 SP1 (includes .Net frameworks 1.1, 2,0, 3.0 and 3.5). No configuration of the .Net Framework is required.
- Microsoft SQL Server 2005 Express Edition, Service Pack 2 must be installed followed by Service Pack 3. Any required configuration of the SQL Server should occur following the installation of the server, once the database for the server has been created.

Note: These components are automatically downloaded from Microsoft by the server installation program if not present at install time. They are also available from Microsoft's website as a download. Microsoft frequently redesigns its websites therefore an Internet download link is not provided. Instead we recommend that you use Google or another search engine to find the download links for the mandatory software. On examining the search results, please ensure that the download source is Microsoft.

Optional Software

- Microsoft SQL Server Management Studio Express – useful for editing database settings.

Before Installing the VSoIP Pro Server

Please read the following sections before installing the VSoIP Pro Server.

All Operating System Settings

The PC should have the operating system installed either by the computer manufacturer or from the operating system installation media. It is assumed that the computer does not belong to any Windows network domain.

Note: Changes to the operating system settings, such as changing the local or global policies relating to rights and permissions, are discouraged. These notes assume that the operating system is set up in a fresh installed state.

A single local user should be added. This should be a member of the local administrator group. Server installation, .Net installation and SQL installation, and all maintenance should be done as this local user with local administrative rights.

Note: The server and SQL database engine run as Windows services and as such will execute irrespective of which user, if any, are logged in to the PC.

To prevent unscheduled system restarts, switch off the automatic Windows update feature. Updates of the Windows operating system should be carried out as a part of scheduled system maintenance.

Networking Settings

- Set up the network settings for the PC and make sure that the PC network connection is enabled and connected. Check this by opening a command prompt and running the `ipconfig` Windows command-line utility, (see Appendix A, "Maintenance Information").

Caution: The surveillance system is designed to work in systems where there is a single active network connection. Multiple network cards require further configuration so are not recommended. The surveillance system is designed to bind to the highest priority (default) network interface. If the system uses a connection other than the intended one, use the operating system's network connection tool to disable all connections other than the one intended to be used, or if other connections are required, e.g. for a NAS network, then use the Advanced Settings dialog of the Network Connections tool to specify that the network used for surveillance video is the top most in the connection order.

- It is worth noting the IP address of the server – this address could be useful for clients that cannot discover the server using the multicast discovery system built into the software system because the network does not support multicast.
- The PC must be set up so that it can browse the Internet. During installation, the server needs to contact a licensing server located on the Internet in order to complete the installation and become licensed.
- The use of the Dynamic Host Control Protocol (DHCP) in the surveillance site is not recommended, as the VSoIP Pro Server will be unable to locate devices if their IP address are reassigned. We recommend that static IP addresses are used at all times.

Firewalls and Port Usage

For best performance, simplicity of setup and easy maintenance, it is recommended that a dedicated firewall protects the entire network rather than firewall software running on the server PC.

Any local software firewalls should either be disabled, or carefully configured so as not to prevent the server from contacting the licensing server. Also, any hardware firewall on the LAN should be configured to allow appropriate network access to the PC on which the server is executing. Some local, software-based firewalls block incoming/outgoing traffic solely on a port number basis. Others block ports to all but explicitly defined applications.

Caution: Blocking required ports and/or not allowing the server and related applications to use the network can prevent successful installation, licensing or execution of the server.

Table 2 details which ports are used by the server. These ports must be open and unused by other applications to ensure that the server works correctly. For information on how to tell if a port is in use, see “Determining PC Port Usage” on page 144.

Table 2 Server application port usage

Application	Role	Default Path	Port number	Description
Setup.exe	Server installer	Installation media	80/TCP	The bootstrap installer for the server
.MSI file	Server installer	Installation media	80/TCP	The main installer for the server
Services.Service.exe	Server Application	C:\Program Files\GANZ\VSoIPSuite Server	25473/TCP	Server service application
LicensingHelper.exe	Server Licensing	C:\Program Files\GANZ\VSoIPSuite Server	80/TCP	Required to license the server
VSoIPService	Server Application	C:\Program Files\GANZ\VSoIPSuite Server	25474/TCP	Server web service
VSoIPService	Mapsets	C:\Program Files\GANZ\VSoIPSuite Server	8080/TCP	Required to view mapsets

More details about port utilisation should be available in documentation supplied with the IP camera or encoder, on the manufacturer's website, or from their technical support contacts.

It is not advisable to execute the following on the server PC unless the impact of their execution is considered carefully:

- Anti-virus.
- Anti-spyware.
- Software firewall.

Switching off Power Saving

By default, many operating systems are set to “sleep” after a specified time period. You should disable **all** power saving related to the computer’s hard drive and monitor displays, including the following:

- Sleep
- Hibernation
- Turn off monitor
- Turn off hard disks
- System standby
- Screen saver

Depending on your operating system, these options may be accessed as part of a power scheme or power plan. Where multiple power plans are available, you should always select one that provides maximum performance.

Caution: It is **essential** that you disable power saving, as entering into power saving mode will stop the VSoIP Pro Server, which in turn will stop some or all recording jobs on the integrated recorder.

Installing the VSoIP Pro Server

1 Log in to the computer using the user name of the local user with administrative level privileges.

2 Navigate to and double-click setup.exe to start installation.

The server installer program setup.exe automatically examines the local system for the .Net Framework and SQL Server Express Edition. If these are not present, or they are earlier versions, the installer program will automatically connect to Microsoft’s servers over the Internet and download the correct versions of the software.

3 Click to accept the terms of the license agreement.

4 Click Advanced to change the default installation folder, if required.

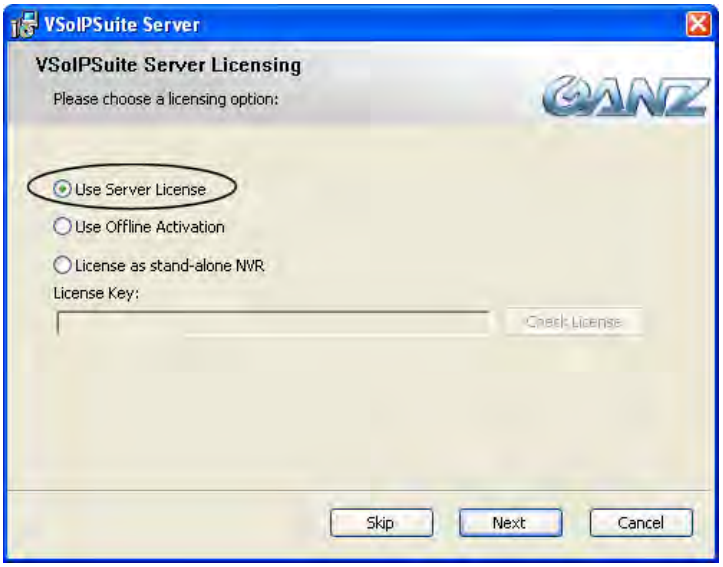


Figure 1 Licensing the VSoIP Pro Server

5 Select Use Server License, and click Next.

Installing the the VSoIP Pro Client on the Same Computer

Although it is possible to run the VSoIP Pro Client on the same computer as the VSoIP Pro Server, this should be avoided in all but the smallest of systems, as it can lead to a conflict of resources.

Offline Licensing

If the computer on which you are installing the VSoIP Pro Server is not connected to the internet, you can still license it, as follows:

1 Select Use Offline Activation during installation, then click Next.

2 Navigate to the folder where you want to save the license data or accept the default and click Save License Data.

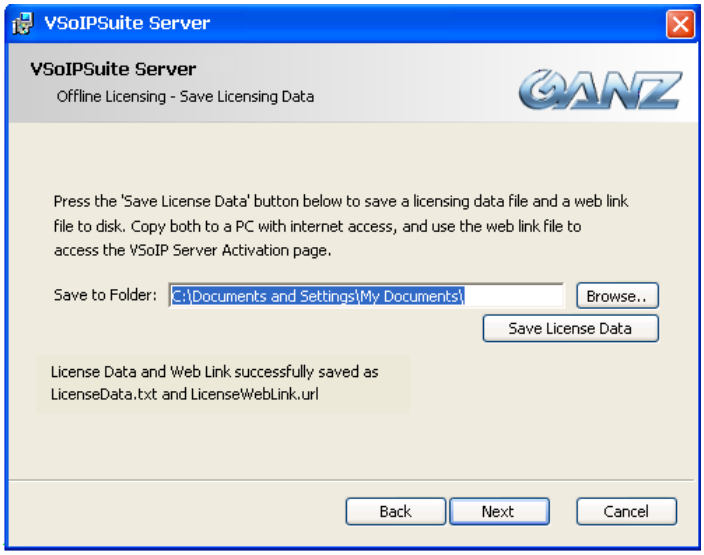

VSoIPSuite Server
VSoIPSuite Server
Offline Licensing - Save Licensing Data
GANZ
Press the 'Save License Data' button below to save a licensing data file and a web link file to disk. Copy both to a PC with internet access, and use the web link file to access the VSoIP Server Activation page.
Save to Folder:
C:\Documents and Settings\My Documents\
Browse..
Save License Data
License Data and Web Link successfully saved as LicenseData.txt and LicenseWebLink.url
Back
Next
Cancel

Figure 2 Saving license data

3 Once you have saved the license data, click Cancel to close the installer. Open Windows Explorer and navigate to where you saved the license data.

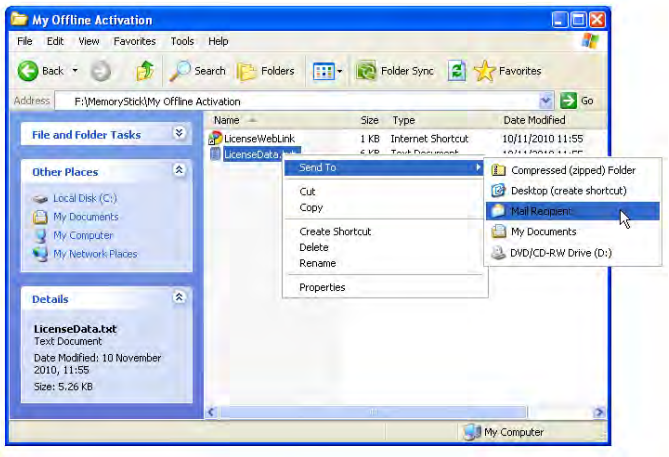


Figure 3 Copying license data

4 Email the LicenseData.txt file and your license key to a CBC Technical Support representative. They will then forward the activated license file to you.

5 Once you have received the activated license file, save the file to your hard drive. Note the name of the file as you will need it later.

6 Open the installer application again, and select Offline Activation as before.

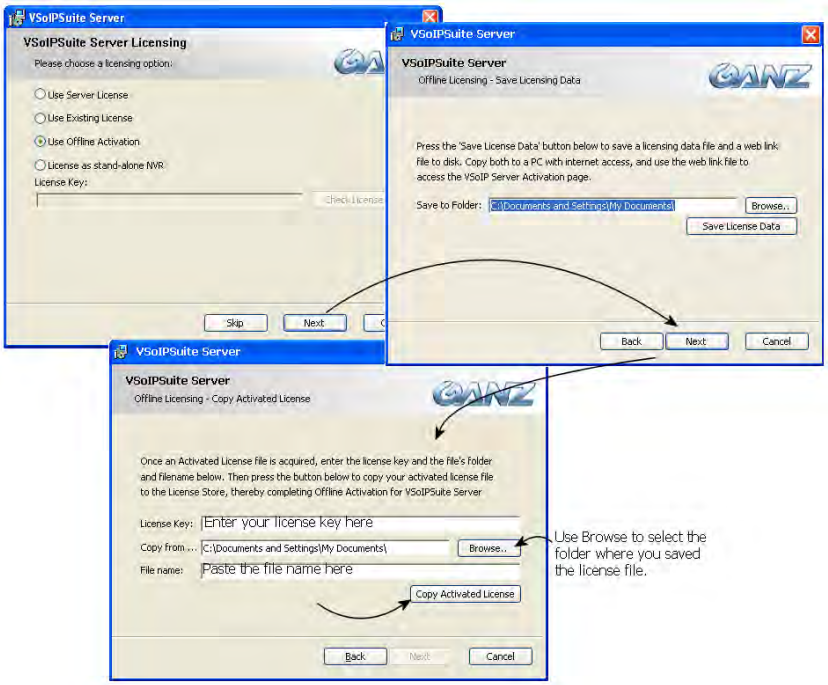

VSoIPSuite Server
VSoIPSuite Server Licensing
Please choose a licensing option:
Use Server License
Use Existing License
Use Offline Activation
License as stand-alone NVR
License Key:
Skip
Next
VSoIPSuite Server
VSoIPSuite Server
Offline Licensing - Save Licensing Data
Press the 'Save License Data' button below to save a licensing data file and a web link file to disk. Copy both to a PC with internet access, and use the web link file to access the VSoIP Server Activation page.
Save to Folder:
C:\Documents and Settings\My Documents\
Browse...
Save License Data
Back
Next
Cancel
VSoIPSuite Server
VSoIPSuite Server
Offline Licensing - Copy Activated License
Once an Activated License file is acquired, enter the license key and the file's folder and filename below. Then press the button below to copy your activated license file to the License Store, thereby completing Offline Activation for VSoIPSuite Server
License Key:
Enter your license key here
Copy from ...
C:\Documents and Settings\My Documents\
Browse...
File name:
Paste the file name here
Copy Activated License
Back
Next
Cancel
Use Browse to select the folder where you saved the license file.

Figure 4 Licensing the VSoIP Pro Server

7 Follow the steps shown in Figure 4.

8 If licensing has been successful, click Next to continue the installation process. If not, see "Installing the VSoIP Pro Server" above for reasons why licensing might have failed.

Using the VSoIP Pro Server

Prior to starting the server, confirm the following:

- Network connection is available and configured.
- You are logged in with administrative privileges.

The server runs as a Windows Service. As such it runs irrespective of whether or not a user is logged into the computer.

Note: Using the PC for other purposes in addition to running the server service might impact on the performance of the server.

The server can be controlled in one of two ways. Either it can be started and stopped manually, or it can be started and stopped automatically when the operating system starts up and shuts down.

Starting the Server Manually

From the Start menu locate the VSoIP Pro Server entry and choose the Start Service option. This signals to the server that it should start up and run as a background task until the computer is shut down. When restarting the computer, the server will not start again unless started through the Start menu.

Figure 5 Starting the server service

Starting the Server Automatically

From the Start menu locate the VSoIP Pro Server entry and choose the Autostart option. This signals to the server that it should start up and run as a background task until the computer is shut down. When restarting the computer, the server will be signalled to start again and to remain running as a background task whenever the computer is running.

Stopping the Server

From the Start menu locate the VSoIP Pro Server entry and choose the Stop Server option. This signals that the server should stop running as soon as possible. If the startup of the server was automatic then automatic start is switched off. The server will now only start when the Start menu>Start Server command is chosen.

Troubleshooting

How can I be sure the Server is running?

The VSoIP Pro Server runs as a Windows service. See Appendix A, "Maintenance Information" for more details. It may not start when commanded, or appear to start but not react when a client tries to use it.

1 Using the Windows services listing application, check the status of the server service.

2 If the server service has not started then check the Windows Event Viewer application to determine what errors might be preventing startup.

Note: Although the system may report that the server service has started successfully, it is possible that the service may have started and then stopped almost at once. If you cannot access the server you should take the steps outlined in Figure 6 which demonstrates a common reason for a server service not starting – the use of an invalid or expired license.

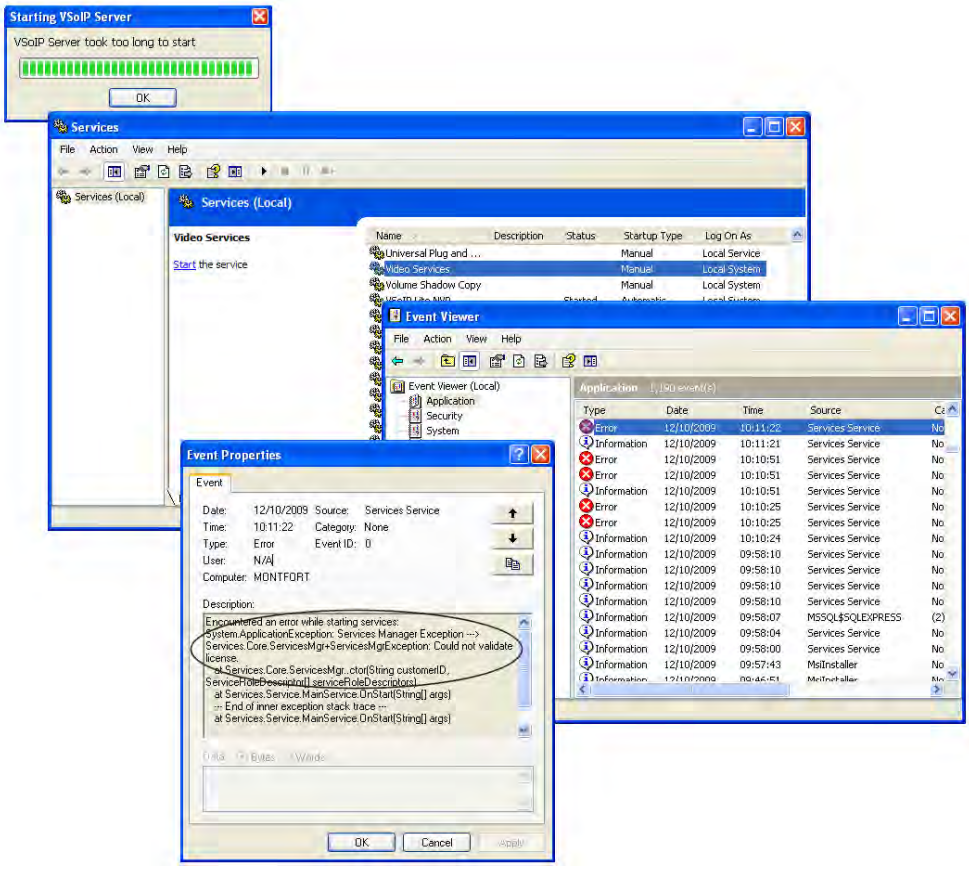


Figure 6 Troubleshooting the server service using Windows application

Network Time Server

It is **extremely important** that all PCs running the client software and other devices use a coordinated time service.

One unified time source must be used. If this coordinated time is provided by the Windows Domain server, then ensure that the source used by the Domain is the same one used for all networked video devices.

If using a Windows Domain controller as a time source, ensure that the Windows Time service is set to automatic start-up.

Chapter 3 – Installing the VSoIP Pro Client

This chapter contains information on the following:

- Prerequisites
- Before Installing the VSoIP Pro Client
- Installing the VSoIP Pro Client
- Post-installation Checklist
- Network Time Server

VSoIP Pro Client Overview

The VSoIP Pro Client software component (the “client”) is a Microsoft .Net framework based application for Microsoft Windows operating systems. It is designed to view live video, play back recordings and monitor alarms originating from surveillance resources such as IP cameras, networked digital video recorders (DVR), computers executing the NVR software component (the “NVR”) and computers executing the Video-wall software component (the “Video-wall”). Access to surveillance resources is controlled by the server software component (the “server”).

The VSoIP Pro Server sends events from various IP cameras, DVRs and NVRs, raising alarms on any client permitted to receive events.

An audit trail representing a historical listing of past surveillance operations managed by the server can be viewed on the client.

Recording tasks such as scheduled recordings can be created and managed using clients. Video footage originating from NVRs within the system can be played back on clients. Access to NVR resources is managed by the server.

The computer used to run the VSoIP Pro Client should not be considered to be a general purpose PC and therefore should not be used for other tasks that might starve the client of system resources.

Caution: It is possible to run a server and/or an NVR on the same computer as the client but this can lead to a conflict of resources and as such is discouraged in all but the smallest of systems.

Caution: Clients discover servers on the network using a multicast-based discovery broadcast. Clients on networks that do not have broadcasting ability must use the IP address of the computer on which the server is executing. Communication between clients, servers and NVRs is via .Net remoting. Communication between clients and Video-walls is via HTTP.

The PC used should be specially tuned for graphical display tasks and should be optimised to have very high Microsoft Direct-X 3D rendering performance. If multi-head displays are being used then it is important to confirm that all heads support Direct-X 3D rendering.

Caution: When using MegaPixel cameras or encoders, the resolution of the rendered image might exceed the Direct-X 3D capabilities of the graphics adapter or driver. Where this occurs, the displayed image will be missing regions of the actual image being sent from the camera and can also be distorted. This is not a fault of the software but is a limitation of the graphics sub-system. Please ensure that the graphics adapter you select can render textures on a Direct-X surface equal to or greater than the resolution of the mega-pixel source.

The network connection bandwidth should be carefully matched to the maximum number of viewing/playback sessions that are likely to be simultaneously viewed. This is the sum of the bandwidths consumed by the video feeds (live/DVR playback/NVR playback).

Prerequisites

This section details the minimum hardware, operating system and software required to run the VSoIP Client.

Note: On large scale enterprise installations, PC specifications should be independently assessed for number of cameras, amount of storage and number of clients. Local conditions should also be taken into consideration.

Hardware Specification

The following is the minimum hardware specification required to provide full frame rate video for 25 streams, without dropped frames, video corruption or latency, for 1 Mbps, 25fps, CIF resolution MPEG4 encoded PAL video with one I-frame every 10 seconds.

Caution: It is highly recommended that you consider the different demands of the bit-rates, resolutions, frame rates, levels of compression and codec types of the system you are implementing when compared with this specification to ensure that your own system has the system performance that matches the demands it is likely to make. In addition, it is wise to add a safety overhead in addition to this to accommodate operating system efficiency changes over time.

- Workstation, architecture 32- or 64-bit.
- CPU 2.4 GHz, or greater (e.g 32 bit Intel Core Quad Core Q6600 Processor 2.4Ghz).
- Memory: 4096MB.
- Hard Drive/Storage - 500GB SATA Hard Drive.
- Optical Drives — DVDROM (for installation) and DVD/RW (for exporting recordings).
- 100 Base-T network card configured for full duplex.
- A high performance graphic system with Direct Draw hardware acceleration and Direct 3D hardware acceleration - such as an nVIDIA® GeForce 9600GT 256MB DDR2 (or equivalent).
- Additional monitors are required to make use of the MultiScreen feature. If you are using more than one monitor, please ensure that your graphics system supports multi-head usage, for example, the nVIDIA® GeForce 9600GT 256MB DDR2 (or equivalent).

Caution: Even on graphics systems with the two types of hardware enabled acceleration, there are some graphics systems that are limited to a maximum number of separate areas of video on-screen that can be supported at the same time. This limitation appears to a user as if no more than a fixed number of video panes can show video, i.e. for those video areas that are not displayed, the application otherwise appears as if the video is being displayed. In this case stopping video which is being displayed in one pane causes the expected video that was not being displayed in another pane to be displayed. This is not a defect in the surveillance client, rather this is a limitation of the graphics system hardware in use.

Caution: When using MegaPixel cameras or encoders, the resolution of the rendered image might exceed the Direct-X 3D capabilities of the graphics adapter or driver. Where this occurs, the displayed image will be missing regions of the actual image being sent from the camera and can also be distorted. This is not a fault of the software but is a limitation of the graphics sub-system. Please ensure that the graphics adapter you select can render textures on a Direct-X surface equal to or greater than the resolution of the mega-pixel source.

Operating System

The recommended operating system is Windows 7 (Pro Edition). The minimum requirement is Windows XP Professional – service pack 3.

Note: The VSoIP Pro Client has been tested and verified on Windows 7 32-bit operating systems. Installation **must** be carried out as Administrator. To run the program, you must right-click VSoIP Pro in the Start menu and select "Run as Administrator".

The VSoIP Pro Client is compatible with Windows 7 64-bit operating systems.

Caution: In geographical regions where different calendar types are used, please ensure that your regional Date/Time setting is set to use the Gregorian calendar.

Additional Mandatory Software

- Windows Installer 3.1
- Microsoft .Net Framework 3.5 SP1 (includes .Net frameworks 1.1, 2,0, 3.0 and 3.5). No configuration of the .Net Framework is required.

Note: These components are automatically downloaded from Microsoft during the installation process if not present at install time. They are also available from Microsoft's website as a download. Microsoft frequently redesigns its websites therefore an Internet download link is not provided. Instead we recommend that you use Google or another search engine to find the download links for the mandatory software. On examining the search results, please ensure that the download source is Microsoft.

- Microsoft Direct-X 9.0c (March 2009) or above. See "Direct-3D Hardware Support and Microsoft Direct-X 9.0c or above" on page 27 for more information on Direct-X.
- Microsoft Internet Explorer version 8 or later (for use with maps and remote access).

  Note: If you intend to use maps with VSoIP Pro, you must add the IP address or network name of the VSoIP Pro Server computer to the list of trusted computers in Internet Explorer. If you don't do this, you may not be able to view camera and alarm icons on your maps. Please see "Adding Trusted Sites" on page 26.

System

A server must be available on the network for a client to operate — if multicast is available on the network the name of the server will be discovered by the client, otherwise the IP address of the server must be known.

Before Installing the VSoIP Pro Client

Please note the following before installing the VSoIP Pro Client.

Operating System Settings

- The PC should have the operating system installed either by the computer manufacturer or from the operating system installation media. The computer is assumed not to be the member of any Windows network domain.

Note: Changes to the operating system settings, such as changing the local or global policies relating to rights and permissions, are discouraged. These notes assume that the operating system is set up in a fresh installed state.

- One local administrator account should be added. This should be a member of the group of local administrators.
- Client installation, .Net installation and Direct-X components installation, and all maintenance should be carried out as this user with local administrative rights.

- To prevent unscheduled system restarts, switch off the automatic Windows update feature. Updates of the Windows operating system should be carried out as a part of scheduled system maintenance.

Networking Settings

- Set up the network settings for the PC and make sure that the PC network connection is enabled and connected. Check this by opening a command prompt and running the `ipconfig` Windows command-line utility; see Appendix A, "Maintenance Information".

Caution: The surveillance system is designed to work in systems where there is a single active network connection. Multiple network cards require further configuration so are not recommended. The surveillance system is designed to bind to the highest priority (default) network interface. If the system uses a connection other than the intended one, use the operating system's network connection tool to disable all connections other than the one intended to be used, or if other connections are required, e.g. for a NAS network, then use the Advanced Settings dialog of the Network Connections tool to specify that the network used for surveillance video is the top most in the connection order.

- The PC must be set up so that it can browse the Internet. During installation, the client will need to contact a licensing server located on the Internet in order to complete the installation and become licensed.
- The use of the Dynamic Host Control Protocol (DHCP) in the surveillance site is not recommended, as the VSoIP Pro Server will be unable to locate devices if their IP address are reassigned. We recommend that static IP addresses are used at all times.

Firewalls and Port Usage

For best performance, simplicity of setup and easy maintenance, it is recommended that a dedicated firewall protects the entire network rather than firewall software running in the client PC.

Any local software firewalls should either be disabled, or carefully configured so as not to prevent the client from contacting the licensing server. Also any hardware firewall on the LAN should be configured to allow appropriate network access to the PC on which the client is executing. Some local, software-based firewalls block incoming/outgoing traffic solely on a port number basis. Others block ports to all but explicitly defined applications.

Caution: Blocking required ports and/or not allowing the client and related applications to use the network can prevent successful installation, licensing or execution of the client.

Table 4 details which ports are used by the client. These ports must be open and unused by other applications to ensure that the client works correctly.

For information on how to tell if a port is in use, see “Determining PC Port Usage” on page 144.

Table 4 Client application port usage

Application	Role	Default Path	Port no	Description
setup.exe	Client installer	Installation media	80/TCP	The bootstrap installer for the client
.MSI file	Client installer	Installation media	80/TCP	The main installer for the client
VSoIPClient	Application	C:\Program Files\GANZ\VSoIPSuite Client	25473/TCP	Access to the server application
VSoIPClient	Application	C:\Program Files\GANZ\VSoIPSuite Client	8080/TCP	Access to the mapset application
VSoIPClient	Application	C:\Program Files\GANZ\VSoIPSuite Client	23109/TCP	Access to the client application (for external PTZ keyboard control)

More details about port utilisation should be available in documentation supplied with the IP camera or encoder, on the manufacturer's website, or from their technical support contacts.

Adding Trusted Sites

If you are using Microsoft Internet Explorer version 8, and intend to use maps with the VSoIP Pro Client, you must add the IP address or network name of the VSoIP Pro Server computer to the list of trusted computers in Internet Explorer. If you don't do this, you may not be able to view camera and alarm icons on map pages displayed in the VSoIP Pro client.

Note: In some surveillance software installations the same operating system login is used for a number of different VSoIP Pro surveillance software users. In this case, the following steps need only to be carried out once for the shared operating system login.

1 Determine **either** the IP address of the VSoIP Pro Server **or** the server's name and domain name. See Appendix A, "Maintenance Information" for more information about determining an IP address.

Note: The IP address or name and domain name of the VSoIP Pro **Client** PC is not required.

For example:

IP Address: 192.168.1.23

Server name and domain name: survellianceserver.organisation.com

2 Log on to the VSoIP Pro Client PC using the user credentials of the user running the VSoIP Pro client software.

3 Do either of the following:

- Open Internet Explorer 8. Click Tools from the toolbar and choose Internet Options.
- Open the Windows Control Panel and choose Internet Options.

4 In the Internet Properties dialog, choose the Security tab. Select the Trusted Sites security zone and then click Sites.

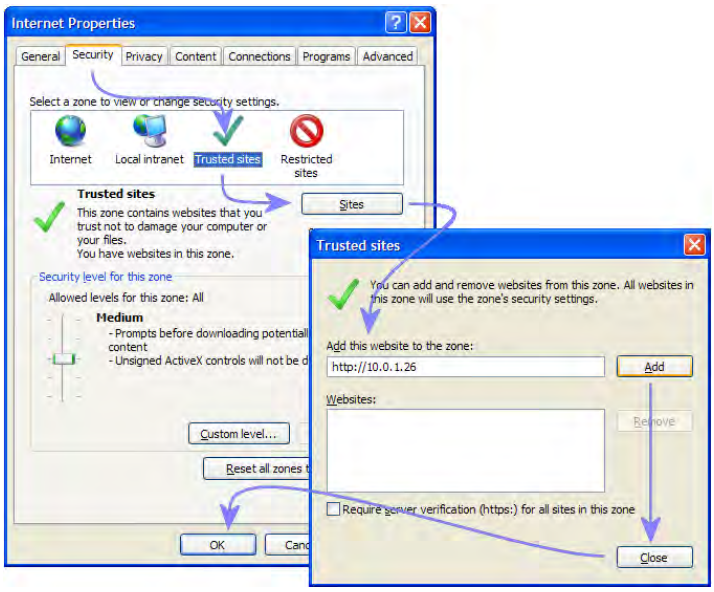


Figure 7 Adding a trusted site

5 In the Trusted sites dialog, type in the IP address of the VSoIP Pro Server or the server's name and domain name, then click Add.

6 Click Close and click OK to submit the changes to the Internet Options.

Additional Security Software

It is not advisable to execute the following on the client PC unless the impact of their execution is considered carefully:

- Anti-virus.
- Anti-spyware.
- Software firewall.

Direct-3D Hardware Support and Microsoft Direct-X 9.0c or above

To ensure maximum performance, the client PC requires an excellent graphic sub-system. The minimum requirement is a graphics sub-system capable of hardware accelerated Direct 3D rendering. You should have also installed the latest released graphic drivers either from the graphic sub-system manufacturer or from the PC manufacturer.

Caution: When using MegaPixel cameras or encoders, the resolution of the rendered image might exceed the Direct-X 3D capabilities of the graphics adapter or driver. Where this occurs, the displayed image will be missing regions of the actual image being sent from the camera and can also be distorted. This is not a fault of the software but is a limitation of the graphics sub-system. Please ensure that the graphics adapter you select can render textures on a Direct-X surface equal to or greater than the resolution of the mega-pixel source.

Note: Some graphic sub-systems are modified to work in the PC manufacturer's hardware.

Use Direct-X diagnostics to determine which version of Direct-X the client PC is using, and whether the graphics sub-system is able to support Direct 3D, as follows:

1 From the Windows Start menu, select Run.

2 In the Run dialog, enter **`dxdiag`**.

3 On the System tab, find the System Information entry for Direct-X version. Check this is version 9.0c (March 2009) or above.

4 On the Display tab, find the Direct 3D Acceleration entry and ensure that it is enabled. If either the version or 3D support is unsatisfactory, the system will be unable to run the client.

Installing the VSoIP Pro Client

1 Log in to the computer using a user name with administrative level privileges; typically this is the administrator user name.

2 Navigate to and double-click setup.exe to start installation.

The client installer program setup.exe automatically examines the local system for the .Net Framework. If this is not present, or it is an earlier version, the installer program automatically connects to Microsoft's servers over the Internet and downloads the correct version of the software.

3 Click to accept the terms and conditions, then click Install.

4 You are then prompted to license the VSoIPSuite Client. You can:

- Use a trial license. Trial licenses allow access to all standard functionality, but after a period of time, text obscures but video panes have text obscuring the video being displayed. If you later upgrade to a full version, you must uninstall the trial client and install the new version.
- Use an existing license from a previous installation (not available for initial installation).
- License the VSoIPSuite Client offline. Use this option if you are installing the clienton a PC with no internet access. See "Offline Licensing" on page 29.
- Enter a new license key to license the VSoIPSuite Client. (Obtain a license key from your vendor).

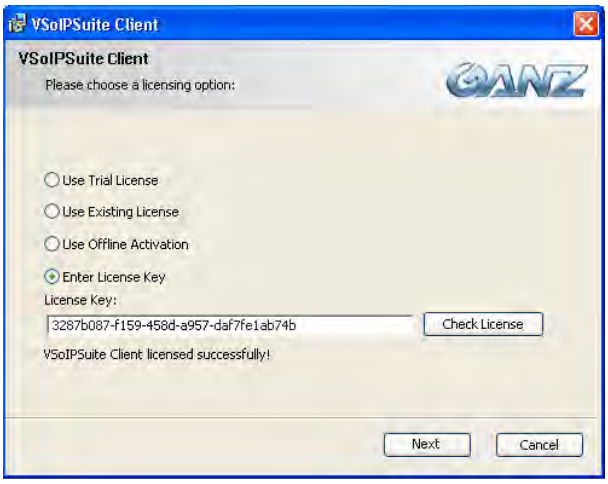


Figure 8 Licensing the VSoIP Suite Client

5 If required, enter the license key you have been given, and click Check License.The key shown in Figure 8 is an example.

The system indicates whether or not licensing has been successful.

If licensing fails, please check the following:

- Have you used the correct license key?
- Has the license key already been used by a different PC?
- Have there been too many hardware changes to the computer?
- Have you turned off the CPU ID feature of your PC or are you using hardware identity masking software? If there are insufficient identifying characteristics, then a license file cannot be generated.
- Are you using machine virtualisation software such as VirtualPC or VMWare? You must use native hardware rather than virtualised hardware.
- Could something be preventing an Internet connection – e.g. firewall block?
- Could the licensing server be busy? Wait a while and try again.
- Do you have sufficient account rights to write the license file to local hard disk? Ensure you are attempting to license the application using an account with administrator level privileges.

- If you are in a geographical region where different calendar types are used, have you set your regional Date/Time setting to use the Gregorian calendar?

Offline Licensing

If the computer on which you are installing the VSoIP Pro client is not connected to the internet, you can still license it offline. The procedure is similar to that for licensing a server offline. See “Offline Licensing” on page 18 for more information.

Post-installation Checklist

Prior to starting the client, confirm the following:

- Network connection is available and configured.
- Microsoft Direct-X 9.0c or later is installed.
- The server is reachable on the network. For more information about how to check connectivity with networked components see Appendix A, "Maintenance Information".
- A “standard user” operating system account has been created, i.e. a member of the Users operating system group.

Network Time Server

It is **extremely important** that all PCs running the client software and other devices use a coordinated time service.

One unified time source must be used. If this coordinated time is provided by the Windows Domain server, then ensure that the source used by the Domain is the same one used for all networked video devices.

If using a Windows Domain controller as a time source, ensure that the Windows Time service is set to automatic start-up.

Starting and Stopping the Client

To start up the VSoIP Pro Client, the VSoIP Pro Server must be running. See “Using the VSoIP Pro Server” on page 19 for information on how to start the server.

Once the server is running, do the following:

1 From the Windows Start menu, select Programs>VSoIPSuite Client>VSoIPSuite Client.

2 The login dialog appears. If your server started up successfully it should be shown — if it is not, select it from the list of servers.

3 The default user name, admin, is shown. Enter the password and click Logon.

Caution: The default administrative password is *admin*. This should be changed as soon as possible as it poses a security risk, should it become known to system users.

Following a successful login, the client remembers the last user name and server used. This allows quicker login next time the client is started. The user’s password is not remembered and must be entered each time the client is started.

To close the client, either:

- Click the X in the top right corner of the application and confirm that you want to shut down, or
- Select at the top left corner, then . Confirm that you want to close the client.

Chapter 4 – Client Configuration

This chapter contains information on the following:

- System Overview
- Getting Started
- User Configuration
- User Group Configuration
- Device Configuration
- Configuring Devices using the Web Interface
- Deleting Devices
- Configuring Video Sources
- Configuring Triggers
- Configuring Pan-Tilt-Zoom Capabilities
- Configuring Audio
- Configuring Sequences
- Audit Trail Configuration

System Overview

The VSoIP Pro system contains several configurable aspects, including:

- Devices — collections of IP cameras, Networked DVRs, Video-walls and NVRs.
- Mapsets — collections of maps.
- System users.
- User groups — groups of users with restricted access to devices, mapsets, and various operations within the system.
- Audit trail — a record of actions taken on the system.

Caution: The incorrect shutdown of the recorder could risk loss of previously recorded footage, or recorder system failure. See “Stopping the NVR” on page 123 for more information.

Getting Started

We recommend that you take the following steps when configuring your VSoIP Pro client:

1 Log in as the default administrative user.

2 Add a new administrative level user.

3 Log out.

4 Log in as the new administrative level user.

5 Change the default administrative user’s password (see “Changing User Passwords” on page 33).

6 Add devices to the system.

7 Add previously constructed mapsets (optional).

8 Add a non-administrative level user group.

9 Assign the devices, mapsets, and set rights and privileges for various actions to the non-administrative level user group.

10 Add all system users to the non-administrative level user group.

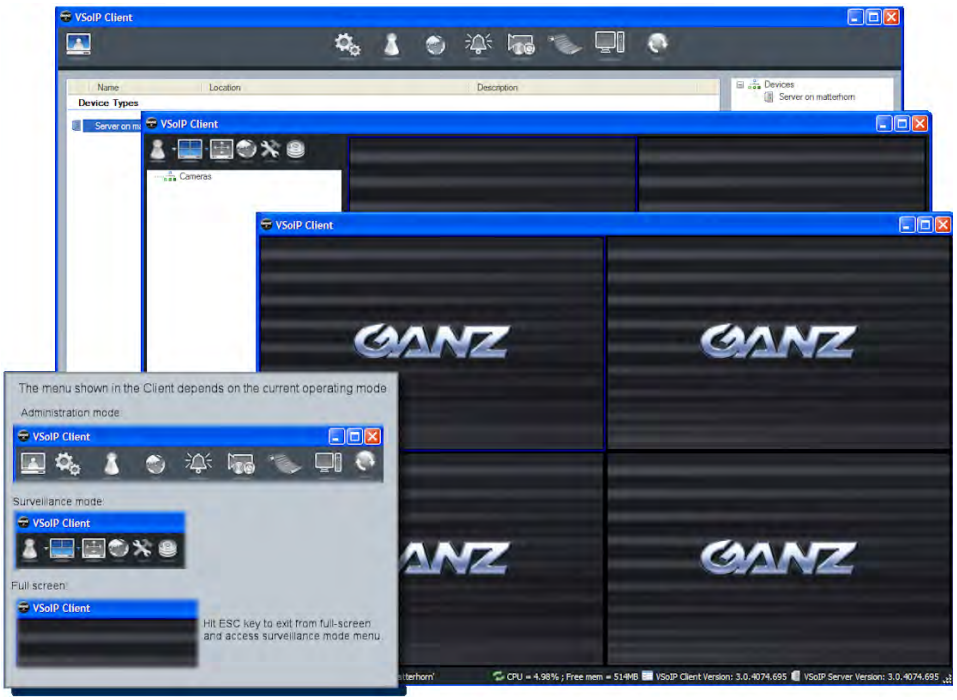


Figure 9 Accessing the client's main menu

User Configuration

By default, each server within the system is preconfigured with one user, the default administrative user. This is the user initially used when starting the system setup process.

Caution: VSoIP Pro is a multi-user system. If you intend having more than one user with administrator privileges, you must set up a separate account for each, rather than providing all administrators with the login details for a single admin account. This avoids system conflicts occurring if two administrators attempt to make changes at the same time.

Note: When you finish adding users, you can create a backup of these in case of data corruption. See "Reusing Devices, Users and Groups" on page 112 for details.

Adding a New User

When adding a new user, you must add the user to an existing group. For more information on groups, see “User Group Configuration” on page 36.

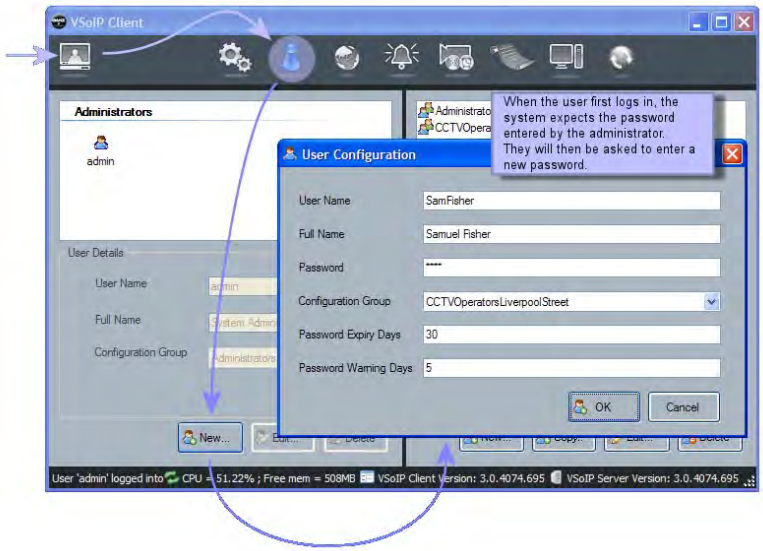


Figure 10 Adding a new user

When setting password expiry details, please note the following:

- Default values are 30 for expiry days and 5 for number of warning days. Change these values as required.
- To create a user with a password that never expires, enter 0 in the Password Expiry Days field. Note that you cannot change this value once set — to change the password timeout you must create a new user.
- If you set the Password Expiry Days field to a non-zero value, you cannot subsequently change this to zero — to set a password that does not expire, you must create a new user.

Setting Passwords for Video-wall and PTZ Keyboard Users

This section applies to you if you are:

- Using a PTZ Keyboard to control VSoIP Pro
- Using VSoIP Video-wall as part of the VSoIP Pro system

In these circumstances, a dedicated user account should be created. This account should have Password Expiry Days set to 0.

Note: If these user account details change:

Keyboard users must reconfigure the software driver with the new account details. Please see “The Software Keyboard Driver” on page 91 for more information.

VSoIP Video-wall and VSoIP Display users should reset the password using the Start menu item (Start>VSoIP Video-wall/Display>Change Login Details) as shown in Figure 11:

Figure 11 Changing the server login details from VSoIP Video-wall

Changing User Passwords

Users with Administrative Privileges

Users logged in with administrative privileges can change the existing password for any user, (with the exception of the default user), as follows:

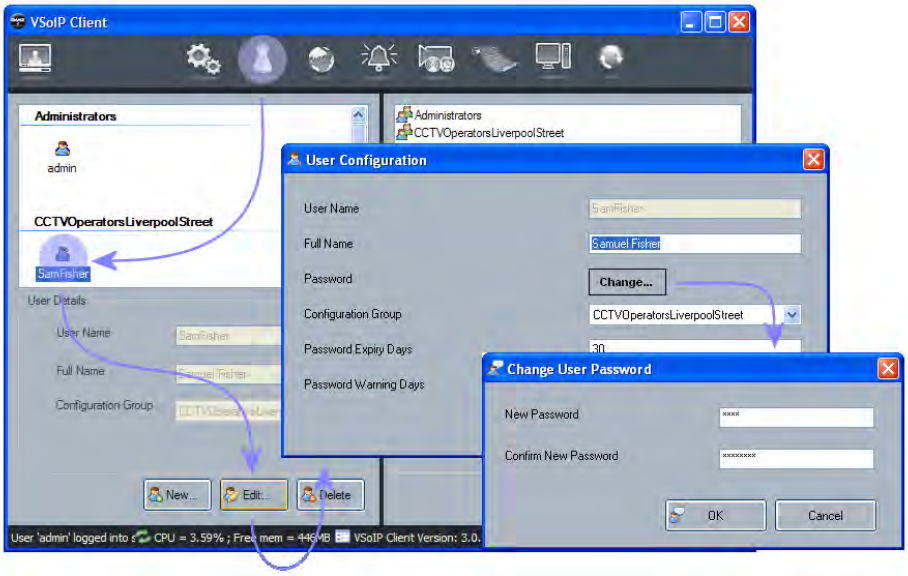


Figure 12 Changing user password

Any User

Any logged-in user (admin or non-admin) can change their password. This method must be used to change the default administrator user password.

1 Select in the top left corner, then .

2 Enter the current password for your user account, then enter a new one and confirm it.

3 Your password is changed. Please keep a note of your password in a safe place.

Temporarily Preventing a User from using a Server

Rather than deleting a user to prevent them from using the system, you can disable the user's log-in privileges.

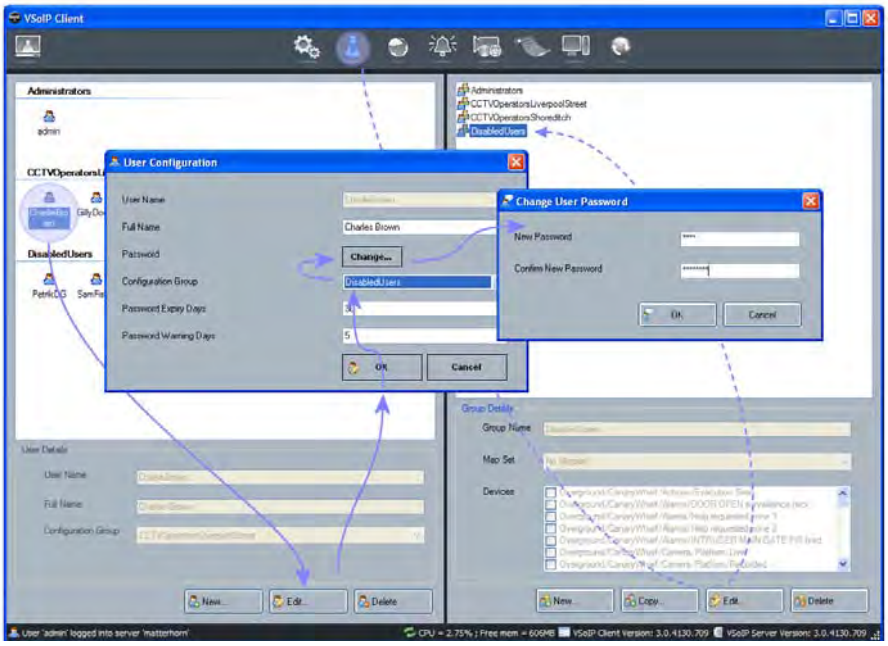


Figure 13 Enabling/disabling a user

To disable a user:

1 Create a Disabled Users group. Members of this group should not have any administrator permissions, nor access to any devices.

2 Select the user to be disabled.

3 Click Edit.

4 Change the group for that user to Disabled Users.

5 Change the password. You now have a group containing users which have been disabled. These users cannot log in since they are unaware of the new password. They would also not be able to access devices, etc, if they were to correctly guess the new password.

Note: It is not possible to disable all administrative level users, i.e. there is always one enabled administrative level user maintained within the system.

Deleting an Existing User

You cannot delete a user if you are logged in on the server as the user you want to delete. You also cannot delete the only administrative user on the server.

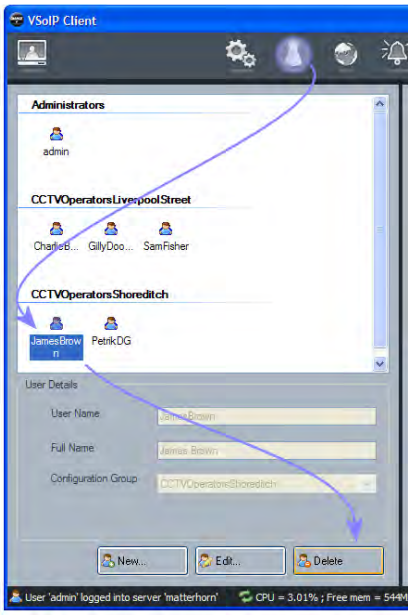


Figure 14 Deleting a user from a server within the system

Logging in as a Different User

Rather than manually closing the application and re-opening it to log in as a different user, you can log in and out in one step, as follows:

1 Select at the top left corner, then . Confirm that you want to log out.

2 The application closes, and a new login box is displayed.

3 Enter the user name and password of the required user.

User Group Configuration

Each VSoIP Pro Server is preconfigured with one user group, the Administrators group. This group provides unrestricted access to the server. Any user added to this group will also gain similar unrestricted access.

Caution: Each server installs one default administrative user with a default user name and password(see page 29). This password should be changed soon after the server is installed and prior to the completion of the system's overall commissioning.

Note: When you finish adding user groups, you can create a backup of these in case of data corruption. See "Reusing Devices, Users and Groups" on page 112 for details.

Creating a User Group

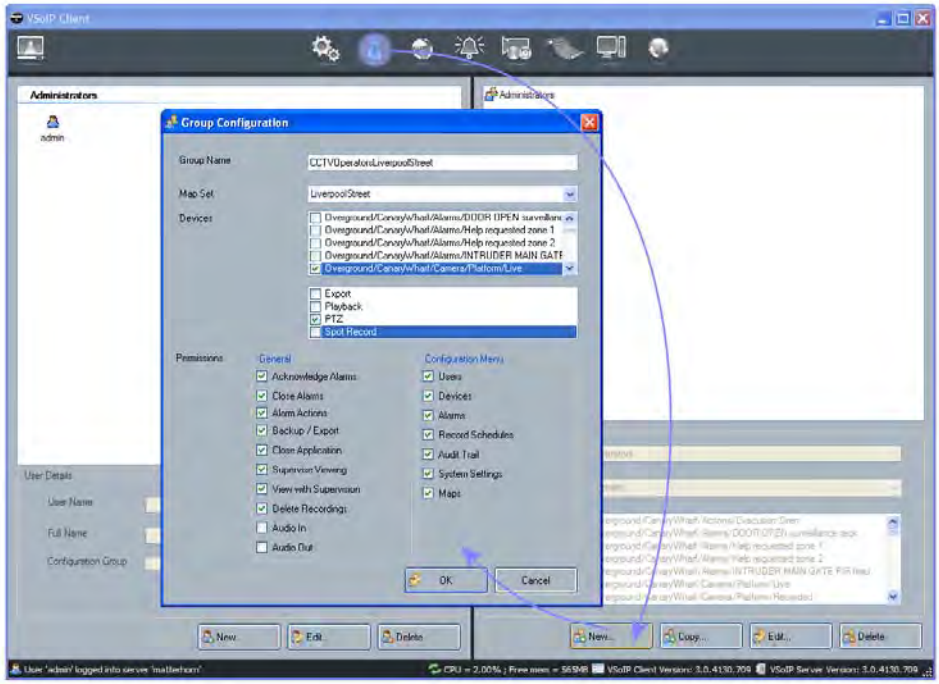


Figure 15 Adding a new user group

To create a new user group:

1 Enter a name for the group.

2 Put a check against those devices that members of this group can access.

Note: Sequences that you have created also appear in this list of devices.

3 Next, for each of the devices, choose the operations in addition to viewing live video that group members can perform. Most of these options are self-explanatory, but the following may need some explanation:

- Alarm Actions — This refers to the Alarm Actions option used with complex alarms (see "Complex Alarm Actions" on page 76). This check box enables/disables client side actions for the logged-in user, for example, the Remote Client Viewing Action.
- Supervise Video — Users belonging to a group for which this is enabled can authorise other users to view recorded video.
- View with Supervision — Users belonging to a group for which this is enabled require another user (with Supervise Video permissions) to authorise them (using their user name and password) to view recorded video. Note that the Playback option for the selected device should remain unchecked. If checked, authorisation is not required to view recorded video.

Note: If both Supervise Video and View with Supervision are enabled for a group, users within this group CAN authorise other users in their group to view recordings, but CANNOT authorise themselves to do so.

4 Next, choose general restrictions that apply to this group, e.g. users in this group are not allowed to create backups of a recording.

5 Finally, specify which administrative operations members can perform, e.g. examine the audit trail, delete users, etc.

6 Click OK.

Copying a User Group

You can quickly create a new user group by copying an existing one and amending its properties as required.

To copy a user group:

1 Select an existing group and click Copy.

2 Enter a name for the new group and amend its properties as required.

3 Click OK to create the new group.

Deleting a User Group

To remove members from a user group, you can delete them or reassign them to a different user group.

Caution: You must ensure that there are no users in a group before you delete it.

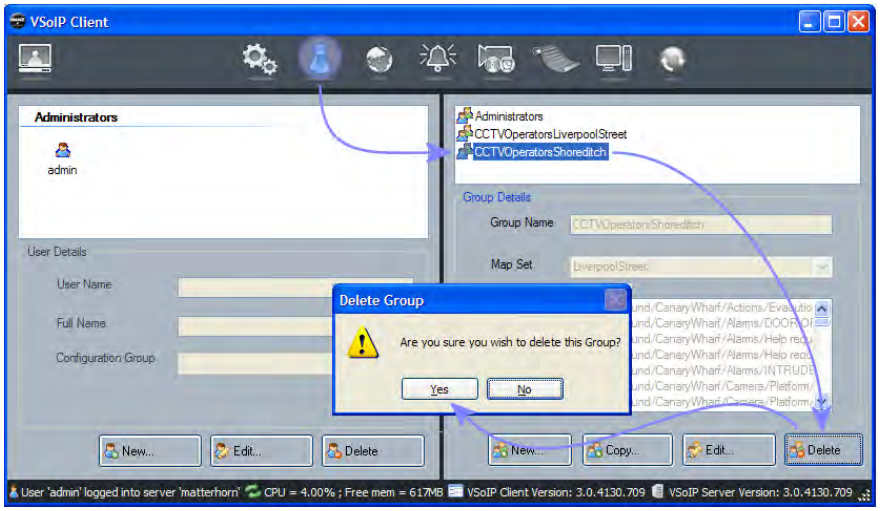


Figure 16 Deleting a user group

Device Configuration

A device can be one of the following:

- An IP camera.
- An IP encoder.
- A Video-wall.
- A Transcode server.
- An Analytic server.
- A Networked DVR.
- A Networked Video Recorder.

Some devices, such as a Networked DVR or an IP encoder can have several analogue camera inputs. In addition, certain devices have multiple encoders for each analogue camera input.

This means that a single device such as an IP camera could generate several video sources, one for each encoder built in to the camera. A Networked DVR can have a number of video sources, typically one for each video input, e.g. sixteen video sources in a sixteen channel Networked DVR.

A Video-wall device is a mirror opposite of devices that act as video sources. A Video-wall displays video sources; the maximum number of video sources displayed at any one time is a fixed capability of the Video-wall device.

An NVR device records video sources and is also a video source. An NVR generates one video source for every playback session that is active.

Some devices support trigger inputs. These are sources that signal that some event has occurred. For some devices this represents a simple electrical voltage being applied to a single input pin. Other signals can be as a result of motion detection events generated by video analytics on the device. NVRs and Networked DVRs can signal the occurrence of a system event such as insufficient storage space, or some other fault.

IP cameras, Networked DVRs and encoders can optionally support Pan-Tilt-Zoom (PTZ) devices. A PTZ device allows the camera's field-of-view to be altered using the pan-tilt-zoom controls in the client.

Note: The surveillance system is preconfigured with a number of types of IP cameras, Networked DVRs, pan-tilt-zoom control units and protocols, NVRs and Video-walls. When you finish adding devices, you can create a backup of these in case of data corruption. See "Reusing Devices, Users and Groups" on page 112 for details.

Adding Devices

There are two methods of adding a device to the server. Many manufacturer's devices can be added using autodiscovery. (This depends on which discovery protocols they support and whether the network allows discovery information to be transmitted.) Those that cannot be added in this way must be added manually.

Note: If using autodiscovery, please note that multicast-based discovery broadcasts used to discover devices or servers will not work correctly when the network connection used has Internet Protocol Version 6 (TCP/IPv6) enabled. Ensure Internet Protocol version 4 is enabled and then disable TCP/IPv6, as shown in Figure 17. On computers where only one Internet Protocol (TCP/IP) is listed then typically this is version 4 and no further modification is required.

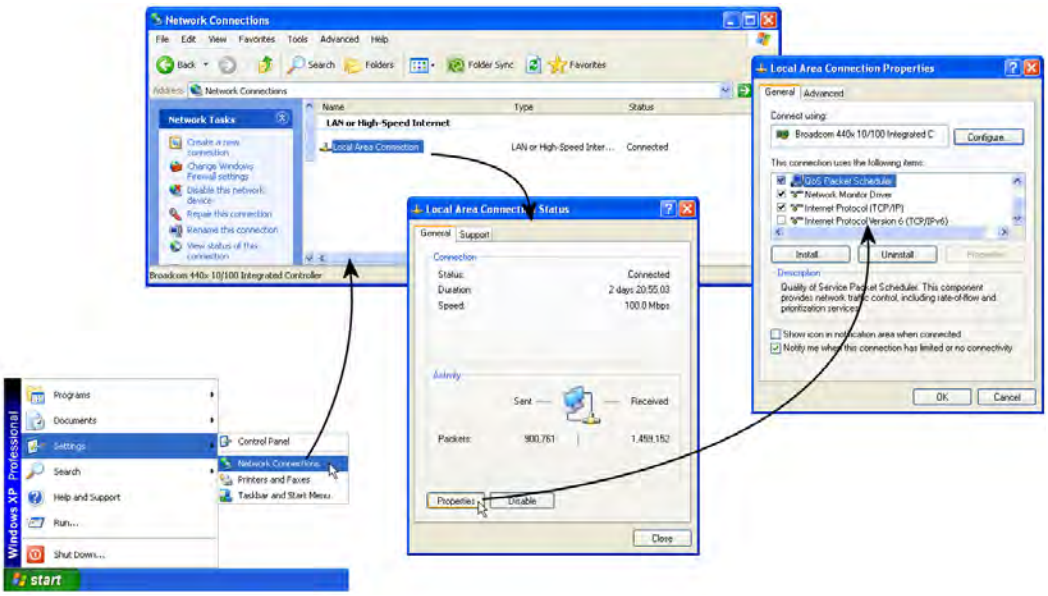


Figure 17 Disabling TCP/IPv6

Adding a Device Using Autodiscovery

VSoIP Pro can perform a scan of the network and list the devices which it finds. Before you start, please ensure Internet Protocol version 4 is enabled (see above). To add a device using autodiscovery, follow the steps shown in Figure 18:

1 A list of all devices discovered on the network is shown. Select the device(s) you require and click the arrow to add them to the site, then click Add, as shown in Figure 18.

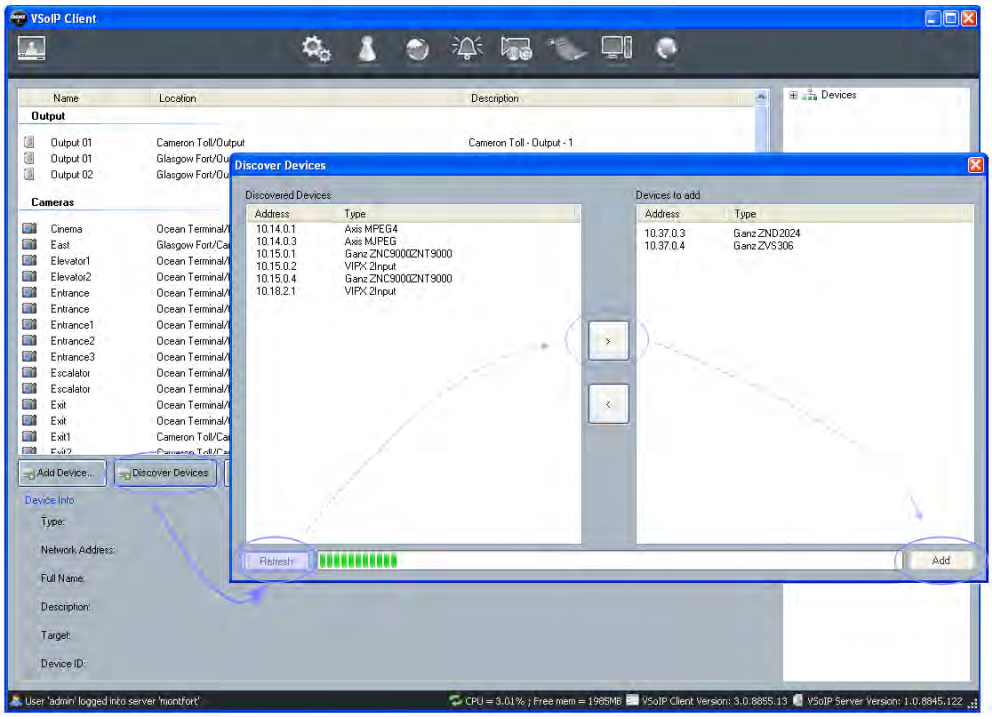


Figure 18 Adding a device using autodiscovery

2 You are prompted to add or amend details for each device in turn that you have added.

Note: Please ensure that the correct codec and transport options are selected for each device (where available), as the default option may not be applicable to all device types.

Adding a Device Manually

If a device has not been discovered by the network scan, you must add it manually as follows:

1 Click Administration, then Add Device.

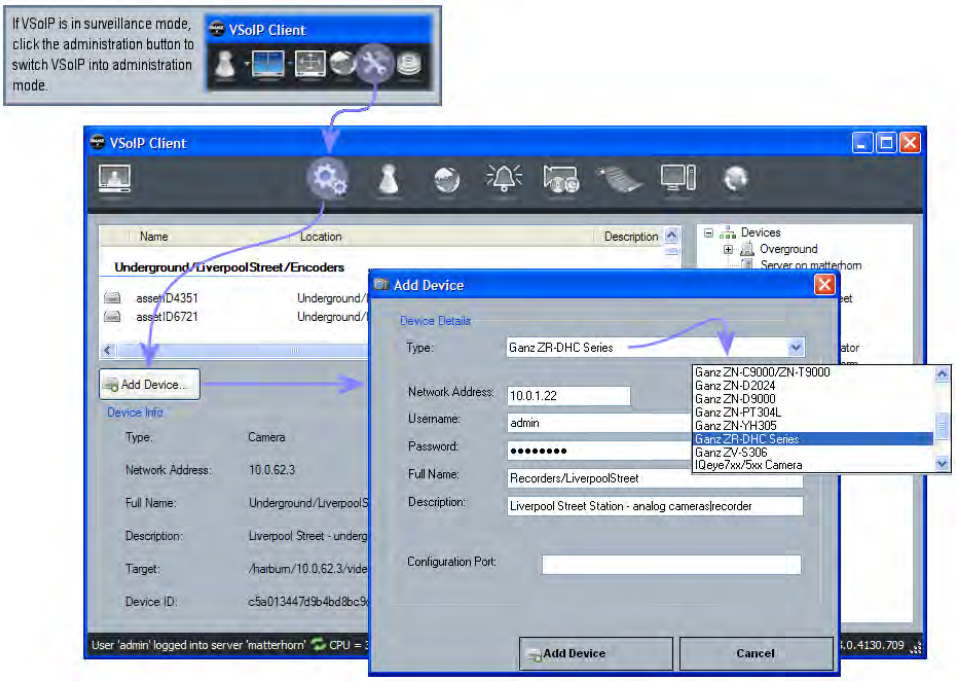


Figure 19 Adding a device

2 Enter a device name and location. Please note that only alphanumeric characters, spaces, forward slash (/) and underscore (_) can be used for the device name.

Caution: When adding an IP camera, encoder or Networked DVR, ensure that the device has been configured so that the device type selected in VSoIP Pro matches the operational parameters of that device.

For example, an IP camera may offer MJPEG, MPEG4 and H.264 as video stream encoding types. If the encoding type has been set to MPEG4 using the camera manufacturer's configuration method, MPEG4 must also be selected when adding the camera to VSoIP Pro. This is done by selecting the correct device type (or sub type) — so for this example, a device type is chosen that matches manufacturer name, device family and that lists MPEG4 as the encoding type.

For example, for the ZN-S1000VE device type, you would choose the MPEG4 option:

ZN-S1000VE	H264
ZN-S1000VE	MPEG2
ZN-S1000VE	*MPEG4*

- If you are adding a device which needs to use a particular port number to support video streaming, eg RTSP, add it after the IP address, in the format 192.168.1.2:554. If you are adding a ZV-S306 camera, please see Appendix C, "Specific Device Considerations" for more information.
- If your device requires a connection URL instead of a simple IP address (for example for ONVIF devices), you should enter this here. See Appendix C, "Specific Device Considerations" for more information on adding ONVIF devices.

- If you are manually adding VSoIP Video-wall or VSoIP Display, ensure that you select the “Videowall 2” option from the drop-down list.

Using Location Text

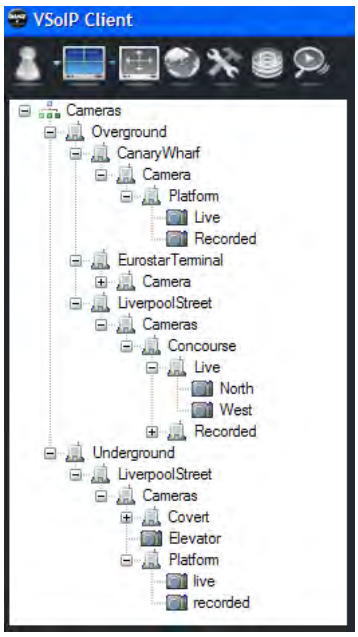


Figure 20 Device hierarchy example

Location text is used to logically group devices. An example of the location text can be seen by looking at the presentation of the device hierarchy or “site”. When constructing a location string each level of the hierarchy is defined by the use of the forward slash character, e.g. ‘/’.

If the location string is left blank then the name of the device is the sole label for the device and is shown at the top level of the hierarchy. A location string entered without slashes adds the device one level down in the hierarchy with a top level entry labelled by the location string. A location string containing two labels separated with a single slash adds the device two levels down the hierarchy, with the text before the slash labelling the device at the top level, the text after the slash labelling the device at the second level and then finally the name of the device labelling the third level.

By naming different devices with common top, second, third, etc location text labels, a number of devices can share some or all of the same location.

Some location text examples as shown in Figure 20:

- Overground (shared with Canary Wharf, EurostarTerminal and LiverpoolStreet)
- Underground (shared with LiverpoolStreet)

Location Text Example

Assume you have a series of video sources with views of different sections of a warehouse.

- Three IP cameras viewing bay one in goods-inward: Cam1, Cam2, and Cam3.
- Two IP cameras in bay two of goods-inward: Cam1 and Cam2.
- Three IP cameras in goods-outward: Cam1, Cam2 and Cam3.

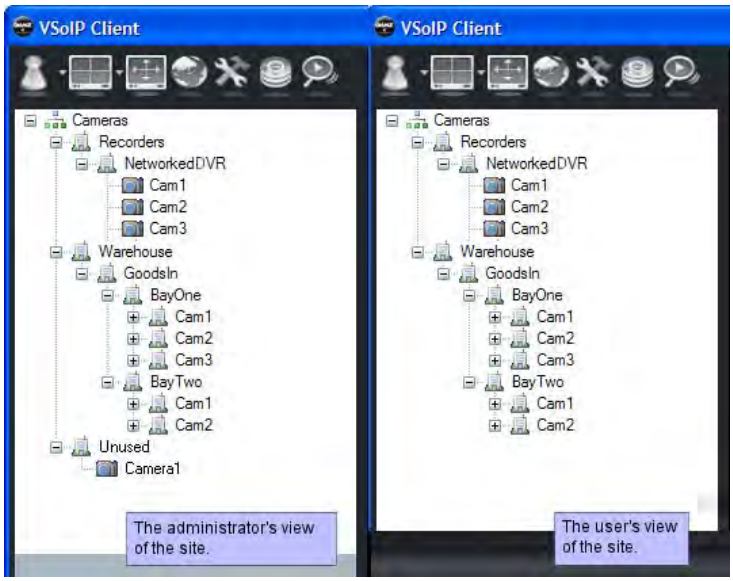


Figure 21 Warehouse site location text example

1 Add three IP camera devices with names Cam1, Cam2 and Cam3 and use the same location text: Warehouse/GoodsIn/BayOne.

2 Next add two more IP camera devices with names Cam1 and Cam2 and use the same location text for both: Warehouse/GoodsIn/BayTwo.

3 Add a Networked DVR device named NetworkedDVR with location text Recorders.

4 Next name inputs 1, 2 and 3 of the DVR Cam1, Cam2 and Cam3 respectively.

Using the name and location text as described above will result in a site as shown in Figure 21.

Using the Location String to Group Unused Devices

Because you cannot delete cameras from a device in the site, you can use the location string to “group” cameras which are currently unused so they can be readily used at a later date.

To do this, create a location string and allocate it to unused devices, as shown in Figure 21. Here, Camera 1 has been given the location string Unused/Camera1.

You can then use the User Group Configuration dialog (see Figure 10) to specify that no users can view devices with that string.

Configuring Devices using the Web Interface

VSoIP Pro allows you to alter a device's configuration once you have added it to the server.

When you add a device to your network, VSoIP Pro receives a configuration URL from the device which allows it to access the device's web-based configuration. If your network has a firewall, you may first need to add a specific port number to this configuration URL to ensure that VSoIP Pro can access the device's configuration page. Figure 22 shows how to do this:

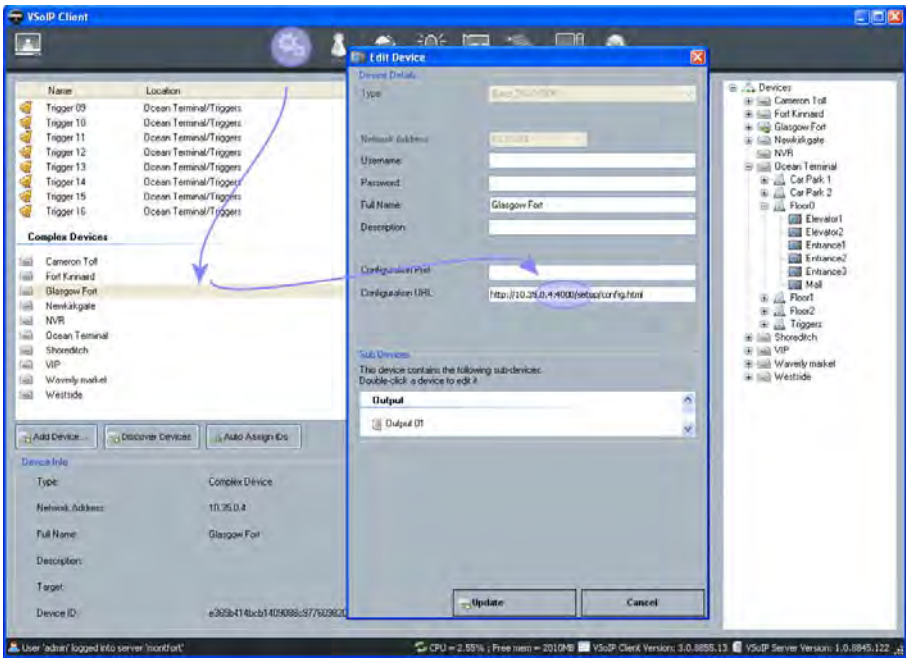


Figure 22 Ensuring device configuration access through a firewall

Once you have added this port number, if required, click Advanced to access the device's web configuration pages.

Note: To configure a device with multiple inputs, ensure that you select the encoder name from the list. For example, in Figure 23, you would select Glasgow Fort.

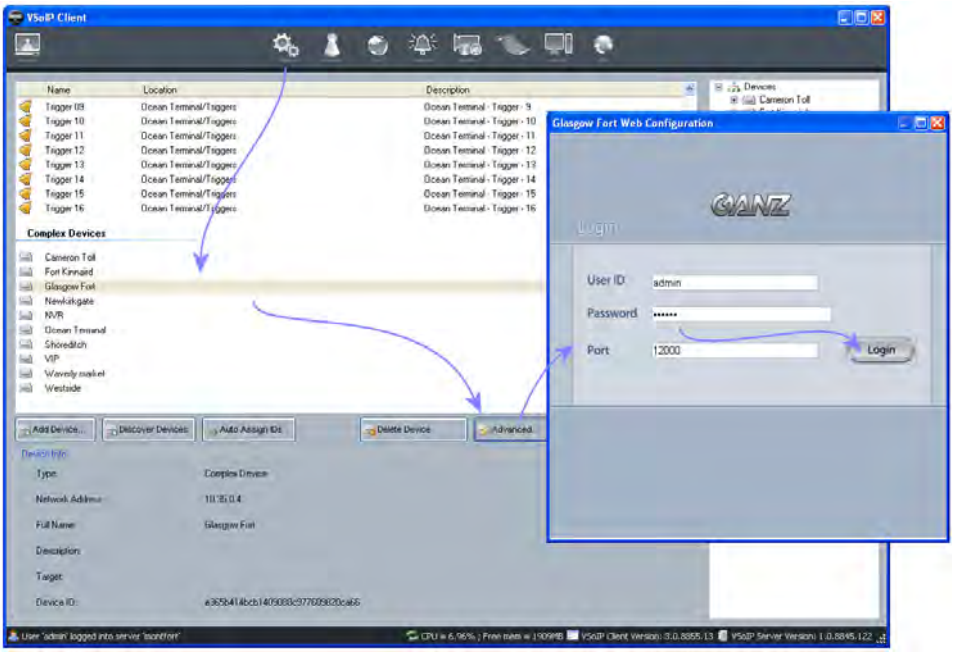


Figure 23 Configuring devices from VSoIP Pro using web page

Deleting Devices

Caution: Before deleting a device, please ensure that the device is not part of any complex alarms, and that no recordings jobs are associated with it. If either of these is the case, please delete these complex alarms and recording jobs before continuing.

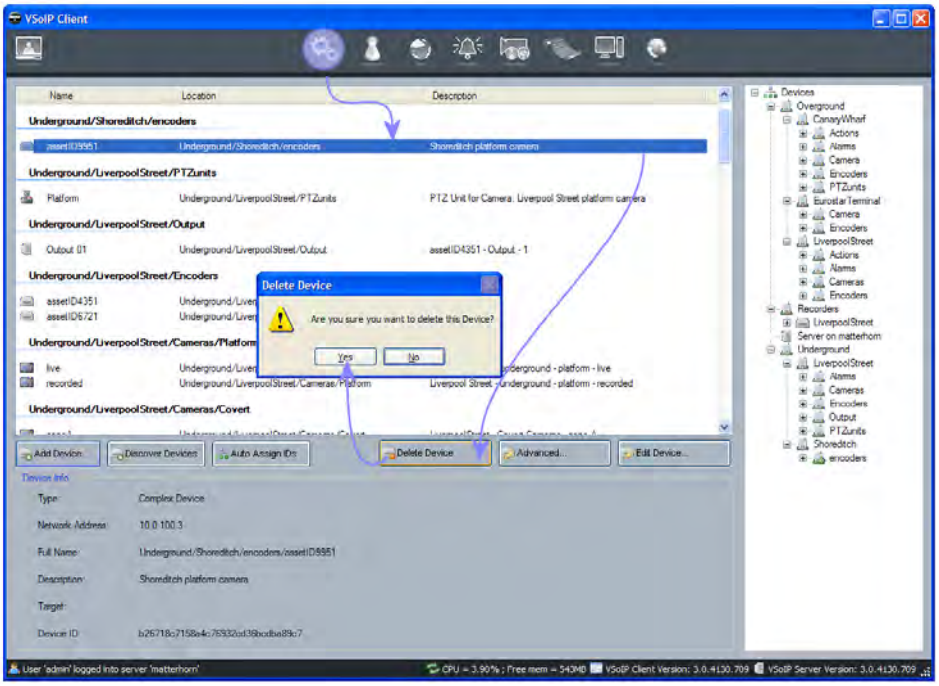


Figure 24 Deleting a device

Note: When deleting a device such as an IP encoder, all associated sub-devices related to that device are also deleted, e.g. PTZ units, etc.

Configuring Video Sources

An IP camera or Networked DVR supports one or more video sources. Each video source has a default name. When a device is initially added to the system, the various video sources are named automatically and grouped into a sub-hierarchy under the device.

The automatically assigned name and location text can be changed, allowing you to group the video sources logically.

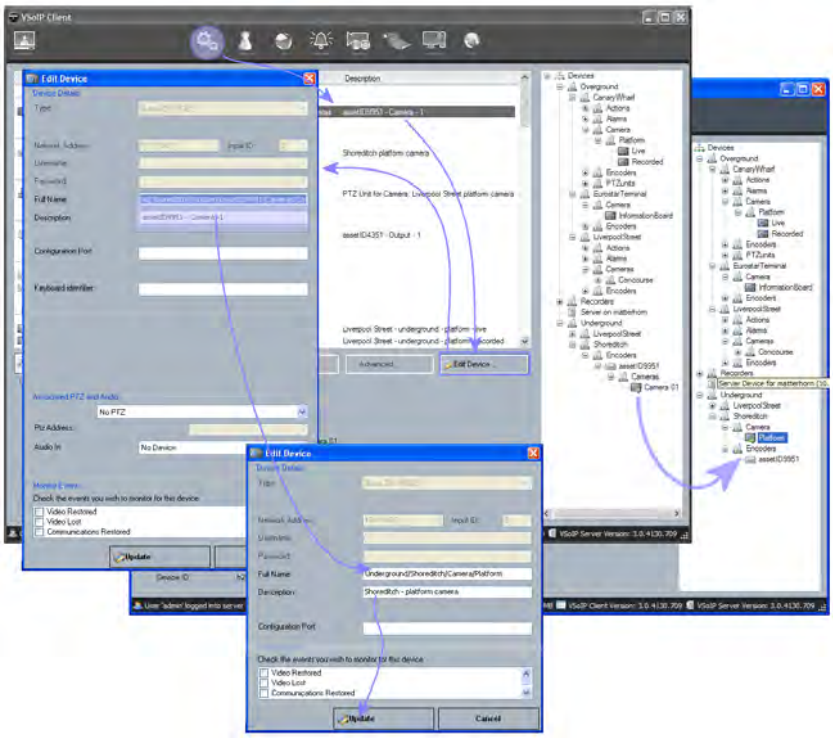


Figure 25 Renaming/setting location for video source

Note: All Networked DVRs can be grouped together in their own logical group of recording devices using the location text. The location text for the various video sources of IP cameras and Networked DVRs can then be renamed and modified to allow the physical layout of the surveillance site to be readily understood from the site/device hierarchy.

Configuring Triggers

A trigger is the source of an alarm, such as an alarm contact on an IP camera or a Networked DVR.

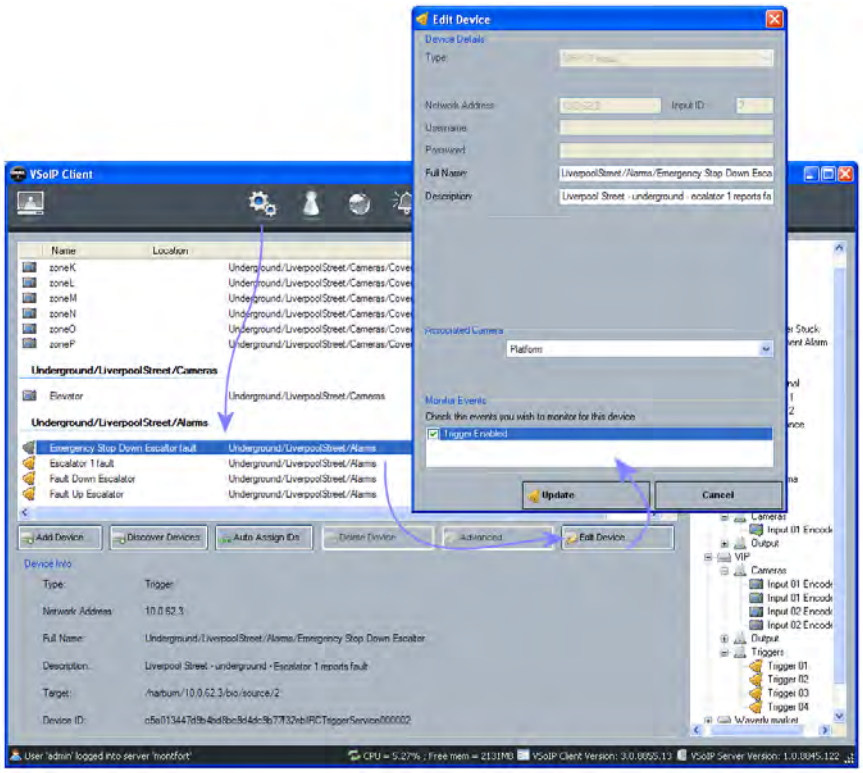


Figure 26 Activating and naming triggers

To activate a trigger:

1 Select the alarm you want to edit from the list and click Edit Device.

2 Select the camera associated with this alarm. This allows operators interacting with the alarm to easily see a related video feed.

3 Check Trigger Enabled. This allows VSoIP Pro clients to receive alarms.

4 Click Update.

Note: There may be a lag time between connection loss of a given device and the raising of an alarm indicating the connection loss. This lag can be anything between 30 and 90 seconds, depending on device and server activity.

Note: Triggers can either be actively monitored or not. When updating a trigger make sure that you have enabled monitoring of events for that trigger.

Use the location text to logically group triggers into groups that make sense for the physical site being monitored.

You cannot delete triggers. If one or more triggers available from a device are not required, then disable monitoring of each trigger event. You can collect unused triggers together under a logical group of unused triggers, keeping them separated from the triggers in use.

Configuring Pan-Tilt-Zoom Capabilities

IP cameras and Networked DVRs can provide connections that enable one or more pan-tilt-zoom control units to be attached. In some cases the IP camera includes a built-in pan-tilt-zoom controller.

The surveillance suite can allow the pan-tilt-zoom control to be controlled by any user within the surveillance site with permissions to do so.

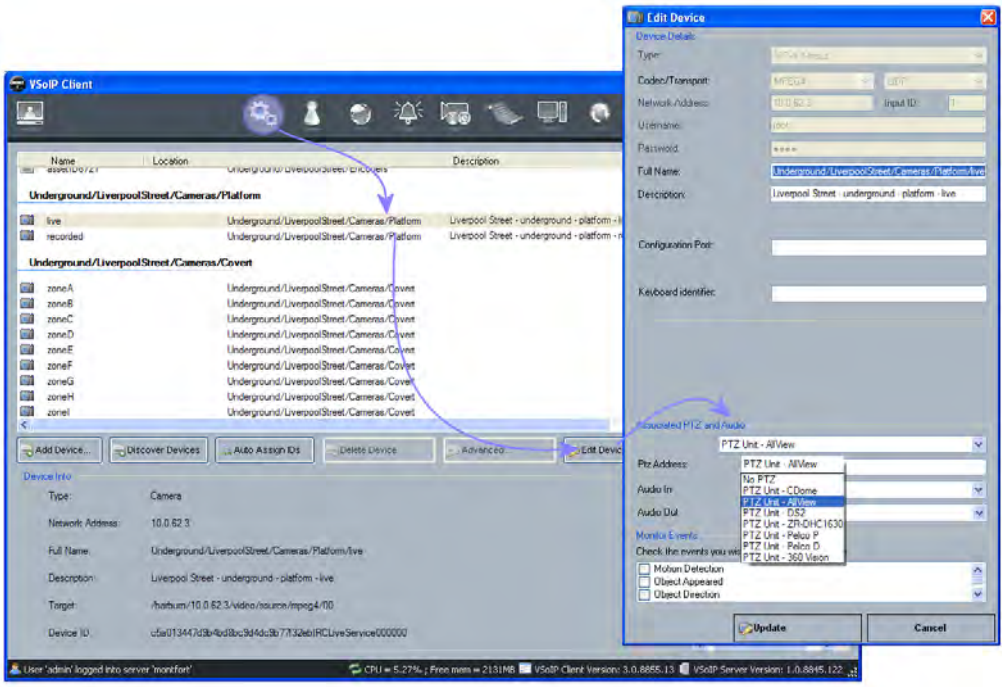


Figure 27 Enabling PTZ capability for a video source

Caution: When you have finished making changes to a device's configuration, you should restart/re-establish any open connections to the device to ensure that the changes take effect.

Some cameras, typically those attached to video encoders, might be connected to a PTZ controller unit. This is usually done using the serial port of the video encoder. E.g. ZN-T9000 connected to a C-ALLVIEW.

A typical arrangement with encoders is to use several analogue inputs alongside several PTZ units. The CCTV installer will use different PTZ addresses when sharing a common serial port.

Under this arrangement, find out the appropriate PTZ address for the camera and PTZ unit pairing and set the appropriate PTZ address when associating a PTZ with an analogue camera.

Configuring Audio

VSoIP Pro supports two-way audio to allow communication with devices which support audio. As shown in Figure 28, audio can either be one way, or both ways between source and destination devices.

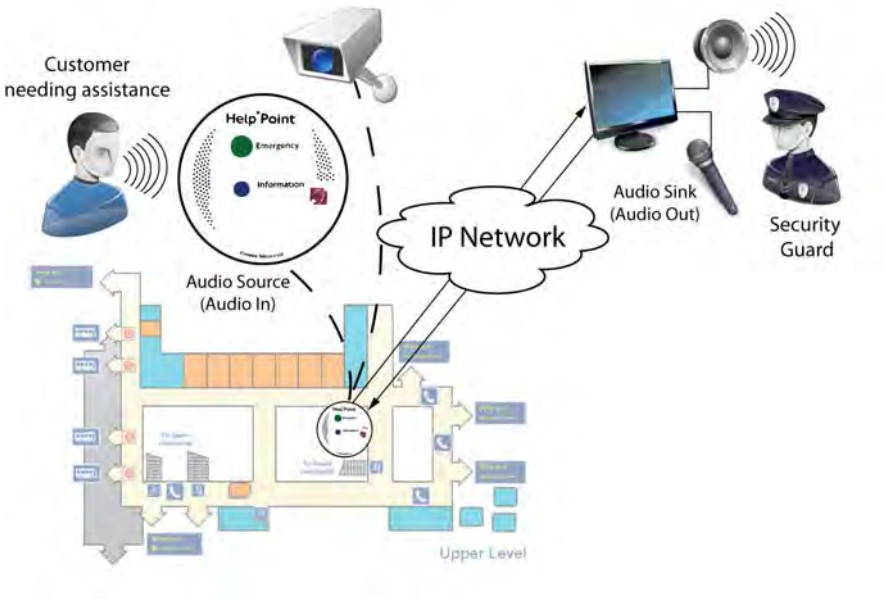


Figure 28 Example of two way audio communication

To configure audio settings:

1 Add an audio-compatible device (see “Adding Devices” on page 38 for information on how to add a device).

2 Select the device you want to configure and click Edit Device.

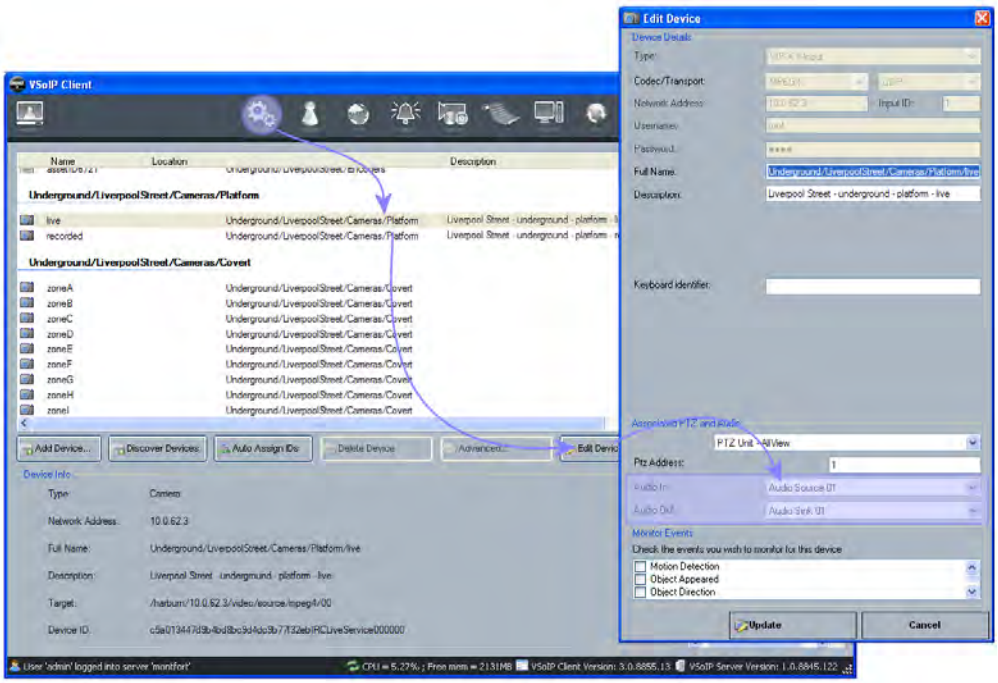


Figure 29 Configuring audio on a device

3 Select the required devices for Audio In and Audio Out respectively (see Figure 29).

4 Click Update to save the settings.

After specifying the audio devices, you can specify how the audio functionality should be controlled within VSoIP Pro. This is configured using the System Settings dialog.

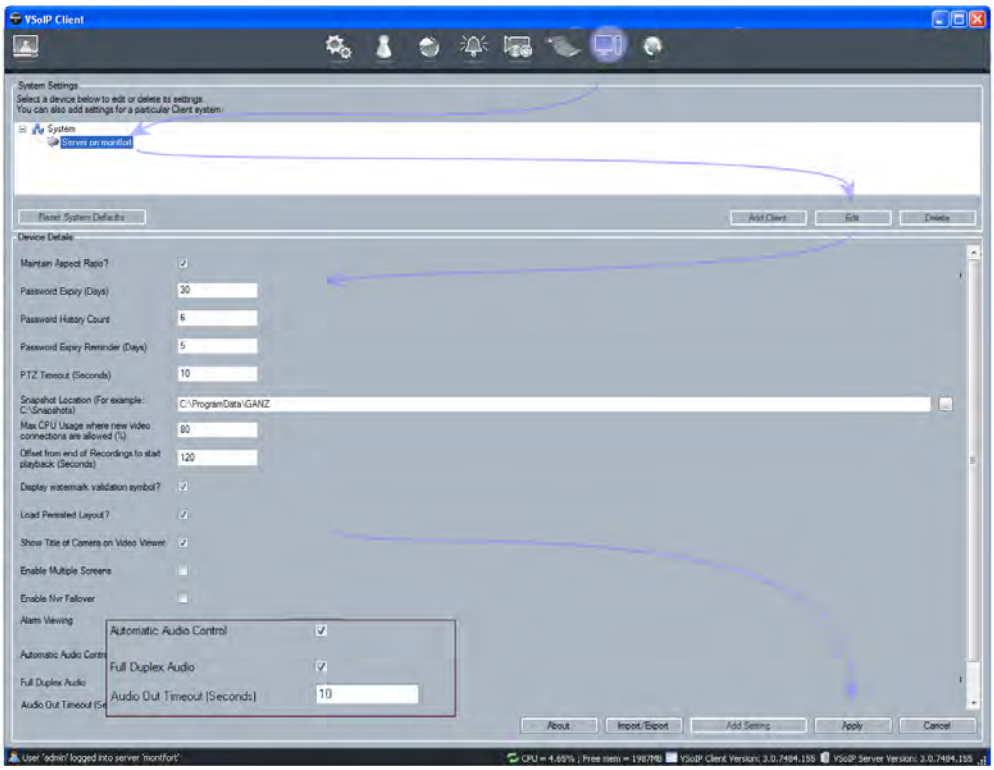


Figure 30 Audio system settings

Caution: When you have finished making changes to a device's configuration, you should restart/re-establish any open connections to the device to ensure that the changes take effect.

Communicating Using Audio

When audio is available for a camera displayed in a video pane, the symbol is shown in the corner of the pane.

Listening to Audio from a Camera

Audio can be used in two modes:

- Automatic

  Select Enabled to use audio in automatic mode. This enables audio in all panes displaying cameras which support audio. Audio is played from the pane which is selected (this may be by clicking on a camera on a map, or simply by clicking a pane which is already displaying video). Changing the selected pane turns off the audio feed in the initial pane, and starts it in the second pane.

- Manual

  Deselect Enabled to use audio in manual mode. You may want to disable Automatic Audio if you frequently switch between panes for other purposes, for example, controlling PTZ cameras. When disabled, you must first select the pane displaying the camera whose audio you want to hear, then click . To listen to audio from a different camera, select the pane playing the second camera, then click again.

Using a Microphone

To use your microphone to communicate with someone on screen, click the appropriate pane and then click . The microphone then remains active until it times out. (See “Audio Out Timeout”, below.)

Preventing Feedback

If you are experiencing feedback when interacting with cameras on screen, disable Full Duplex Audio (Figure 30).This sets the audio mode to Half-Duplex — allowing communication in both directions, but in only one direction at a time.

Audio Out Timeout

This value specifies how long a microphone can be used for before the connection times out.

Configuring Sequences

Note: A sequence is a group of cameras which are displayed sequentially within a single video pane, either on a client or on a Video-wall, each for a configurable length of time. Any number of cameras can be added to a sequence. In order to use a sequence, the currently logged in user must belong to a user group which has permission to view that sequence. See “User Group Configuration” on page 36.

To create a sequence:

1 Select Sequences in the Administration pane, as shown in Figure 31.

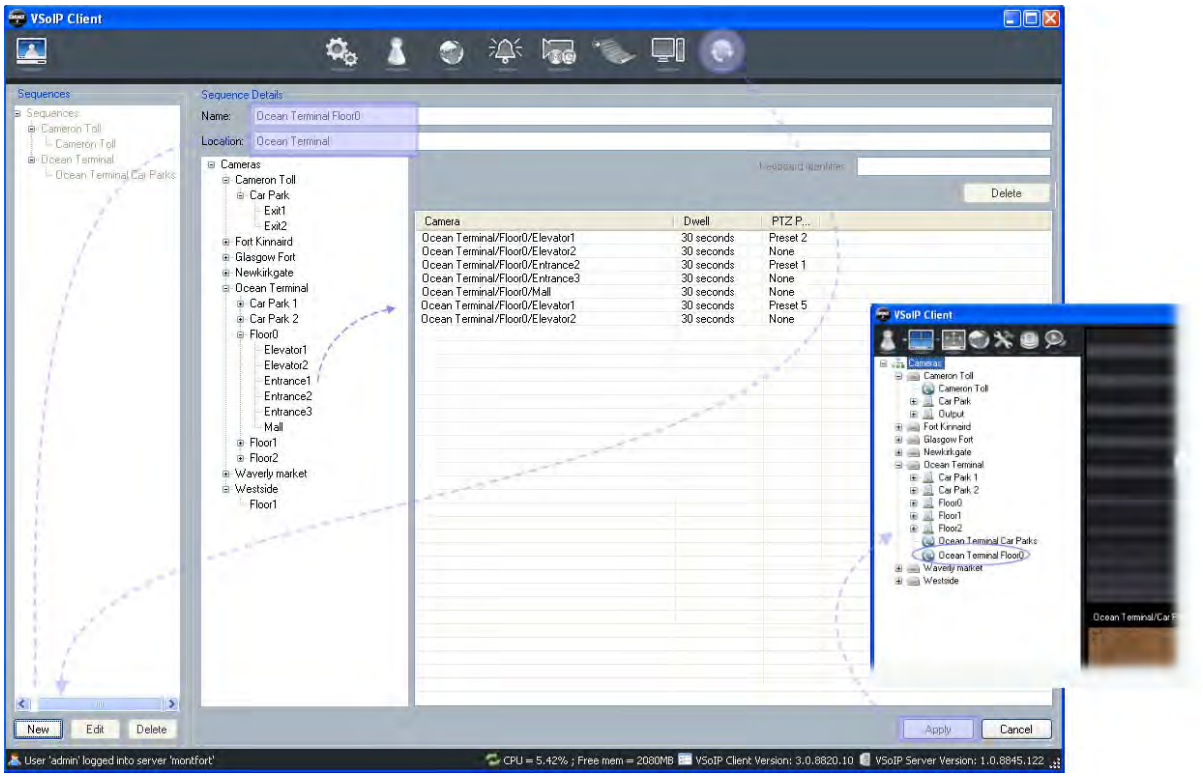


Figure 31 Creating a sequence

2 Select New.

3 Enter a name and location for the sequence.

4 Enter a keyboard identifier if required (for use with a PTZ keyboard).

5 Select a camera in the sequence tree and drag and drop it into the sequence.

Note: Individual cameras can be added more than once to a sequence.

6 Alter the dwell time if required to change the length of time footage from each camera remains on screen.

7 Select a PTZ preset, if required.

Note: If you are associating sequences which use PTZ presets with alarm actions, please be aware that there may be a conflict between the sequence preset and other complex action PTZ preset requests.

8 Add all required cameras, then click Apply.

Note: To edit or delete an existing sequence, select the required sequence in the list and click Edit or Delete, as required.

Configuring PTZ Keyboard Support

For information on working with PTZ keyboards, please see Chapter 9, "Using PTZ Keyboards with VSoIP Pro".

Chapter 5 – Using VSoIP Pro to Monitor your Site

This chapter contains information on the following:

- Working with Live Video and PTZ
- Stored Views
- Working with Alarms
- Playing Back Recorded Video
- Exporting Recorded Video
- Audit Trail Configuration
- Complex Alarm Configuration

Working with Live Video and PTZ

VSoIP Pro allows CCTV operators to view live video from up to 36 IP cameras, cameras attached to networked DVRs and cameras attached to IP encoders. It also allows the operator to move pan-tilt-zoom (PTZ) cameras, to zoom in closer to the scene displayed, and to take a snapshot of a particular moment. The video panes making up the operator's viewing area can be laid out in various ways as suits the operator's needs and the capabilities of the display hardware.

Note: No more than 36 combined live views or playback views may be active at any one time. An error message is displayed if you attempt to view more than this number.

Note: Permissions to view an IP camera, a camera input of a Networked DVR and control a PTZ unit associated with those cameras are managed by the server.

Live Video Controls

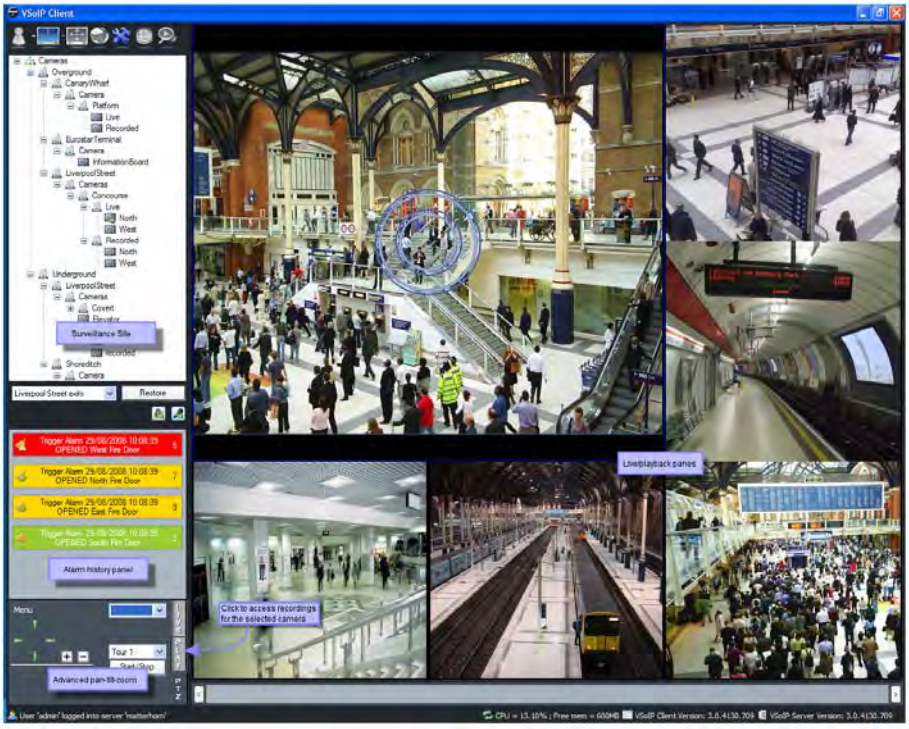


Figure 32 Main live viewing controls

Accessing other features

The main menu can be used to switch the client into various surveillance modes. This menu also allows the operator to change their own password and exit the application.

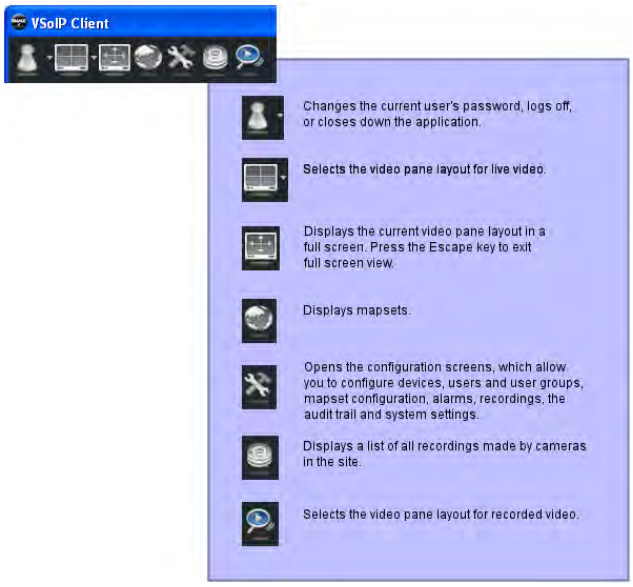

VSoIP Client
Changes the current user's password, logs off, or closes down the application.
Selects the video pane layout for live video.
Displays the current video pane layout in a full screen. Press the Escape key to exit full screen view.
Displays mapsets.
Opens the configuration screens, which allow you to configure devices, users and user groups, mapset configuration, alarms, recordings, the audit trail and system settings.
Displays a list of all recordings made by cameras in the site.
Selects the video pane layout for recorded video.

Figure 33 Location of main menu

Multi-head Monitor Support

VSoIP Pro supports the use of multi-head monitors. See “Default Settings” on page 115 for details of how to enable this support.

Specifying Video Pane Layout

VSoIP Pro offers many different video pane layouts. If you have more than one monitor, you can select the layout for each monitor separately.

To specify a video pane layout, click and select the required layout from the drop down menu.

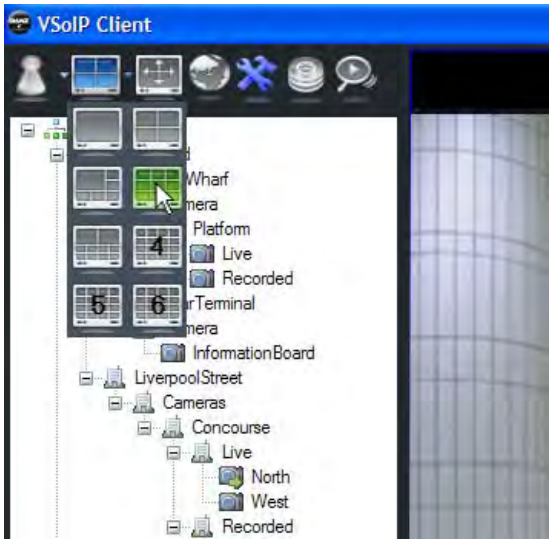


Figure 34 Specifying video pane layout

Double-click any pane to maximise it. Double-click again to restore it to its original size.

If you have a multi-head monitor setup, click at the top left of the additional monitors and select the required layout.

Starting and Stopping Live Video

Figure 35 Starting video using mouse drag-drop

To start video in a video pane, either on the main monitor, or on an additional monitor (if you have a multi-head setup), select the camera in the tree and drag and drop it onto the required video pane. To activate relevant functions for the camera in that pane (for example, PTZ functionality), click once in the video pane. Alternatively, select the pane before dragging and dropping a camera into it.

Figure 36 Stopping video or exiting from a map

Using Digital Zoom

VSoIP Pro allows you to zoom in on and move around live video footage.

Figure 37 Zooming into live video

Right-click the video pane and select Digital Zoom. Click the part of the pane that you want to see in more detail, then use the mouse scroll button to zoom in and out as required. While zoomed in, click away from the centre of the image and drag the mouse to pan the video.

Taking a Snapshot of Live Video

VSoIP Pro allows you to capture snapshots of live video playing in a video pane. These are saved to \Desktop\VSoIP Image Clips\FromLiveDevices, as .jpeg images. To change this location, see “Default Settings” on page 115.

To take a snapshot, right-click in the pane displaying the video at the point you want to capture, and select Snapshot.

Figure 38 Taking a snapshot of live video

Control of Pan-Tilt-Zoom

Activation/Deactivation

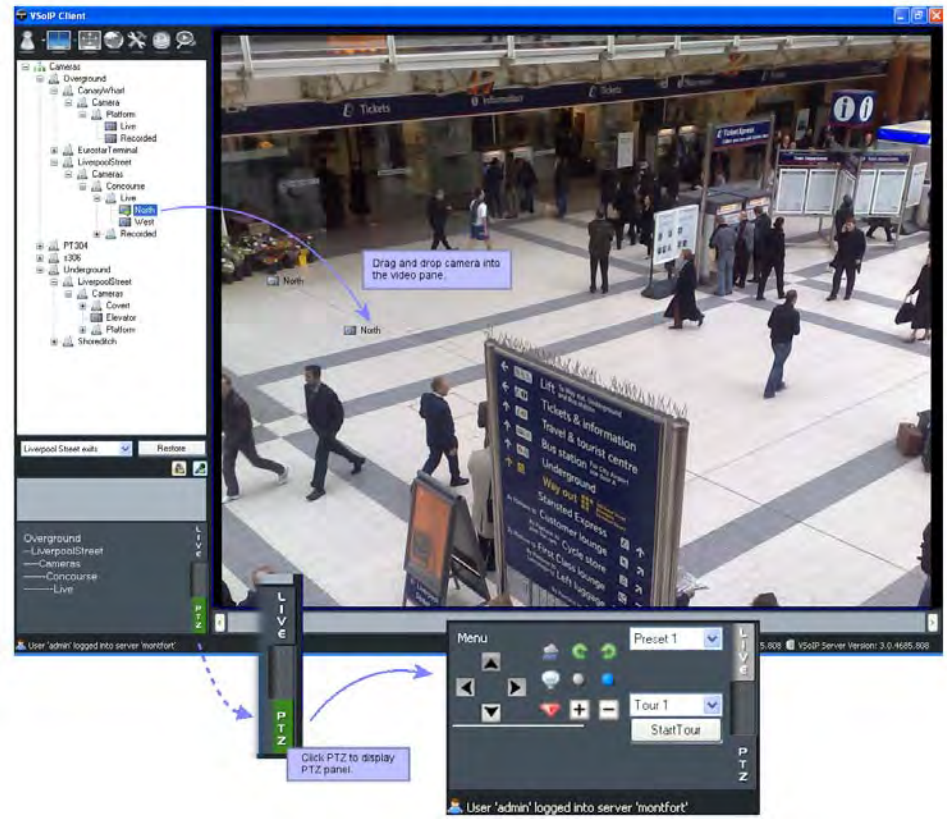


Figure 39 Activating/deactivating PTZ support

Moving and Zooming

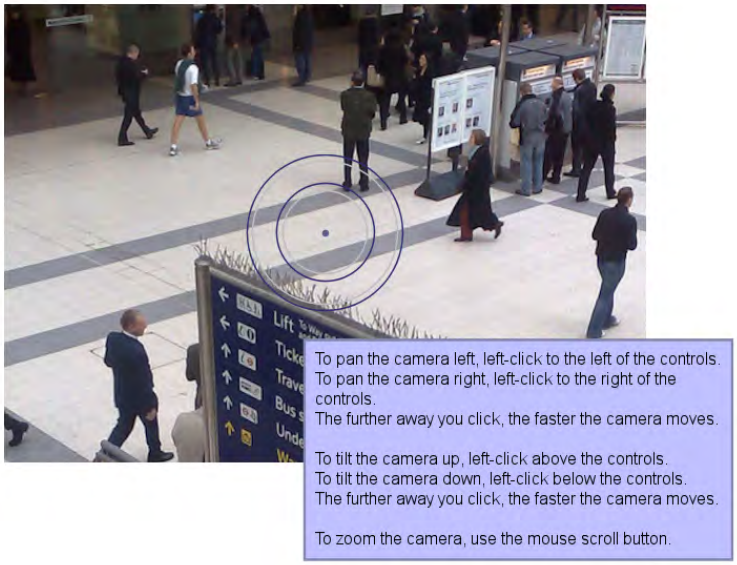

To pan the camera left, left-click to the left of the controls.
To pan the camera right, left-click to the right of the controls.
The further away you click, the faster the camera moves.
To tilt the camera up, left-click above the controls.
To tilt the camera down, left-click below the controls.
The further away you click, the faster the camera moves.
To zoom the camera, use the mouse scroll button.

Figure 40 Panning, tilting and zooming

Extra features

Some PTZ cameras and protocols provide access to extra functionality, which allows you to carry out extra commands, such as using presets or tours. These are detailed below.

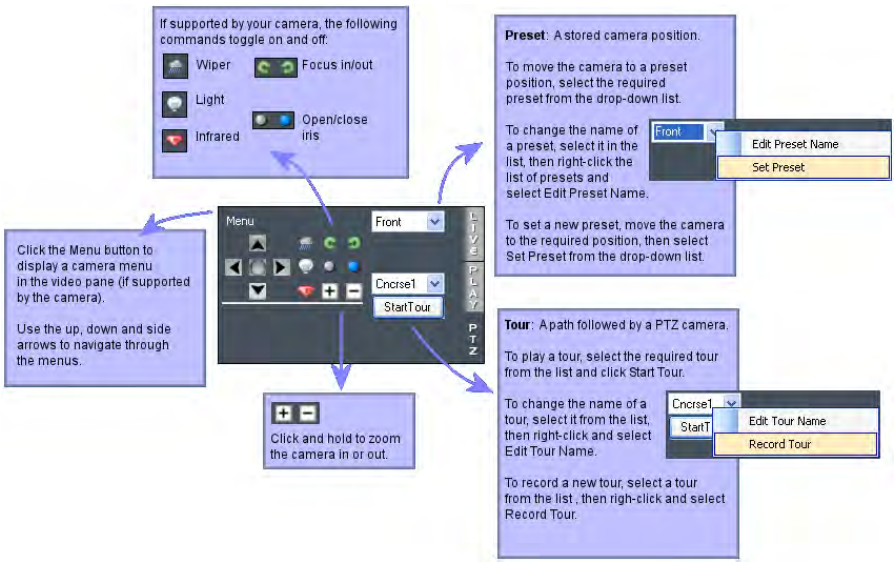

If supported by your camera, the following commands toggle on and off:
Wiper
Focus in/out
Light
Open/close iris
Infrared
Preset: A stored camera position.
To move the camera to a preset position, select the required preset from the drop-down list.
To change the name of a preset, select it in the list, then right-click the list of presets and select Edit Preset Name.
Front
Edit Preset Name
Set Preset
To set a new preset, move the camera to the required position, then select Set Preset from the drop-down list.
Click the Menu button to display a camera menu in the video pane (if supported by the camera).
Use the up, down and side arrows to navigate through the menus.
Menu
Front
Cncrse1
StartTour
LIVE
PLAY
PTZ
Click and hold to zoom the camera in or out.
Tour: A path followed by a PTZ camera.
To play a tour, select the required tour from the list and click Start Tour.
To change the name of a tour, select it from the list, then right-click and select Edit Tour Name.
Edit Tour Name
Record Tour
To record a new tour, select a tour from the list , then righ-click and select Record Tour.

Figure 41 Additional PTZ unit features support

Note: PTZs vary in functionality, so access to features depends on the chosen PTZ unit's capability.

Viewing Sequences

Sequences display a loop of continuous video from different cameras within a video pane. For information on how to set up sequences, see “Configuring Sequences” on page 50.

Note: In order to use a sequence, the currently logged in user must belong to a user group which has permission to view that sequence. See “User Group Configuration” on page 36.

To view a sequence:

1 Navigate to the sequence you want to view in the tree.

2 Drag and drop the sequence into a video pane (Figure 42).

Figure 42 Viewing a sequence

Caution: Before setting up or using a sequence, you should first calculate the maximum bandwidth consumed by the three highest bandwidth consuming cameras in the sequence. For example, your sequence might include a single 2Mbps capped H264 stream from a GANZ ZN-S100V, a 768 kbps capped MPEG4 stream from a GANZ ZN-T9000, a 1.5Mbps capped H.264 stream from a Ganz PixelPro camera and a 2.3Mbps MJPEG stream from a GANZ MP1A camera. In this case, the worst-case bandwidth attributable to the sequencing pane in the client would be 2048 + 1536 + 2356 = 5940Kbps or 5.8Mbps.

To stop a sequence, right-click the pane in which the sequence is playing and select Disconnect.

Stored Views

VSoIP Pro allows you to re-create particular video pane layouts, and to display the IP cameras and camera inputs of Networked DVRs in the panes occupied when the view was stored.

Note: Although all users can access stored views, only users with permission to modify system parameters can add or delete them. When restoring a view, only cameras that the user has permission to view are displayed. All others are not displayed.

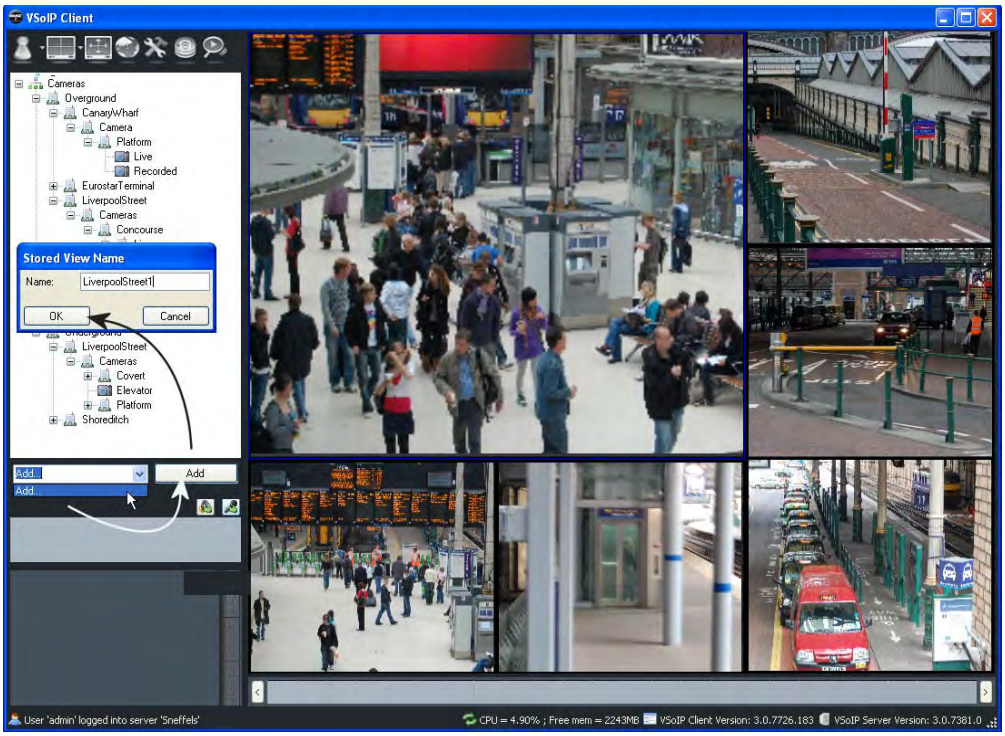


Figure 43 Storing a view

1 Choose the required pane layout.

2 Display the required cameras on the main screen and on any additional monitors you may be using (if using a multi-head setup). If you are displaying a sequence in a video pane, this can also be included as part of the stored view.

3 From the drop-down list, select Add...

4 Click Add.

5 Enter a name for the view.

6 Click OK.

Note: You can save the map view as part of a stored view, but not an individual map. The latest map to be accessed is displayed when the stored view is used.

Updating a Stored View

To update the pane layout or the cameras displayed in a stored view:

1 Select the required view in the list.

2 Change the layout or cameras as required,

3 Click Update. You are asked to confirm that you want to update the view — click OK.

Deleting Stored Views

To delete a stored view:

1 Right-click the name of the view you want to delete.

2 Select Delete.

3 Click OK when prompted to confirm the deletion.

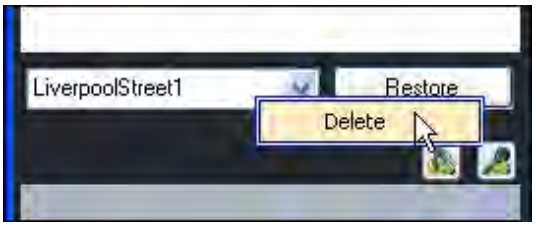


Figure 44 Deleting a stored view

Recovering a Previously Stored View

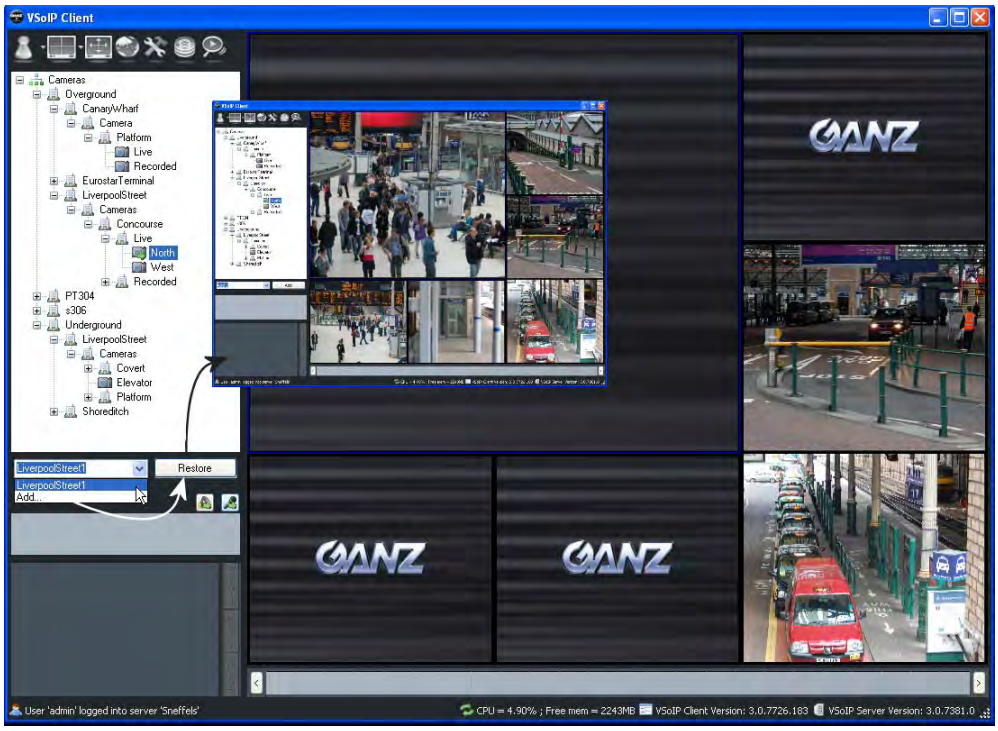


Figure 45 Retrieving a stored view

To retrieve a stored view:

1 Select the required stored view from the drop-down list.

2 Click Restore.

3 The cameras saved in the stored view are displayed.

Note: There is no need to stop video in any pane prior to opening a stored view.

Working with Alarms

The alarm display presents unacknowledged, acknowledged and closed alarms.

Note: To enable the client to display an alarm for a particular alarm source, e.g. contacts on a Networked DVR, the alarm type for the device associated with the alarm source must have been enabled. Access to the device associated with the alarm source must also have been enabled for the group to which the logged-in user belongs. For details, see “Configuring Triggers” on page 46.

Overview of Alarm Display

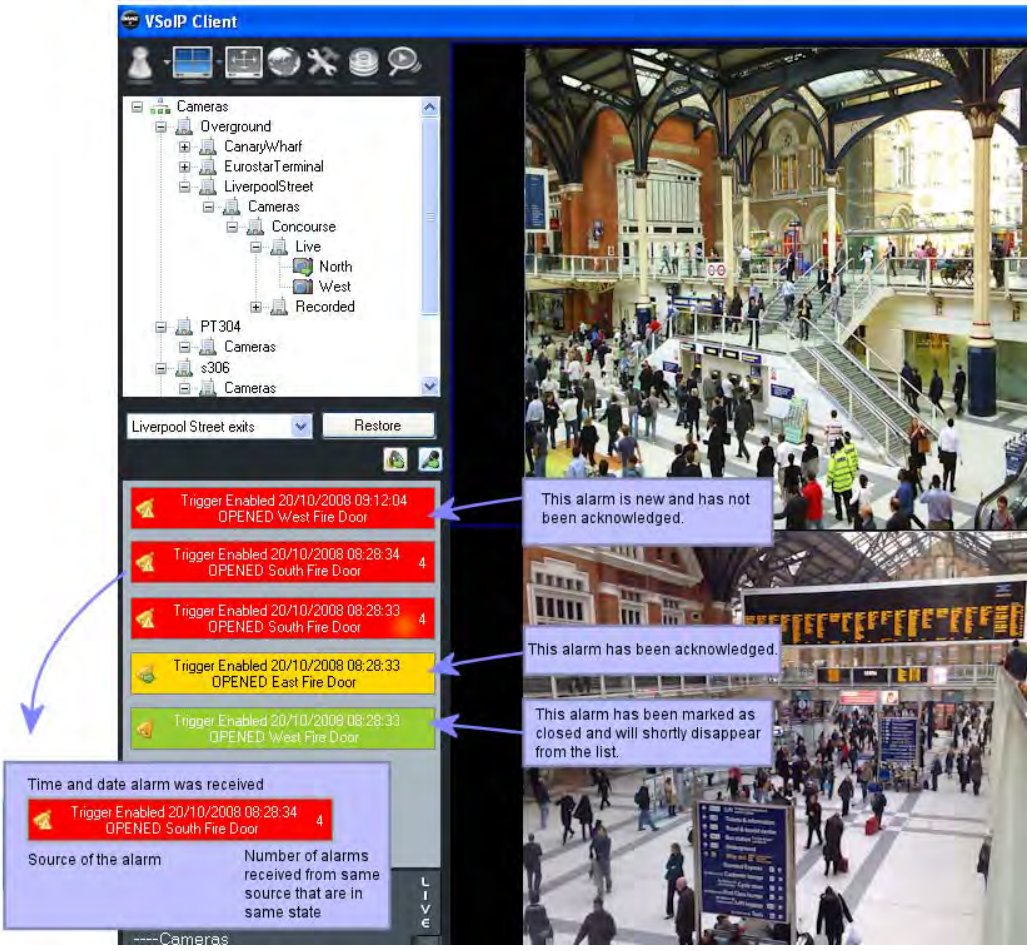


Figure 46 Overview of alarm display

Note: If an alarm in the alarm stack is associated with a camera, you can drag and drop it onto a video pane to view live video from that camera. Similarly, if an alarm in the alarm stack has a recording associated with it, drag and drop it onto a video pane to start viewing that recording.

Viewing Properties of an Alarm

Figure 47 Alarm properties

Note: As shown in Figure 47, the time shown in the tool tip may vary from the time displayed for the alarm. Where possible, the tool tip displays the time the alarm was generated at its source, whereas the alarm entry displays the local time.

Note: There may be a lag time between connection loss of a given device and the raising of an alarm indicating the connection loss. This lag can be anything between 30 and 90 seconds, depending on device and server activity.

Acknowledging an Alarm

Alarms can be acknowledged manually by a user, or automatically by the client.

Manual Acknowledgement

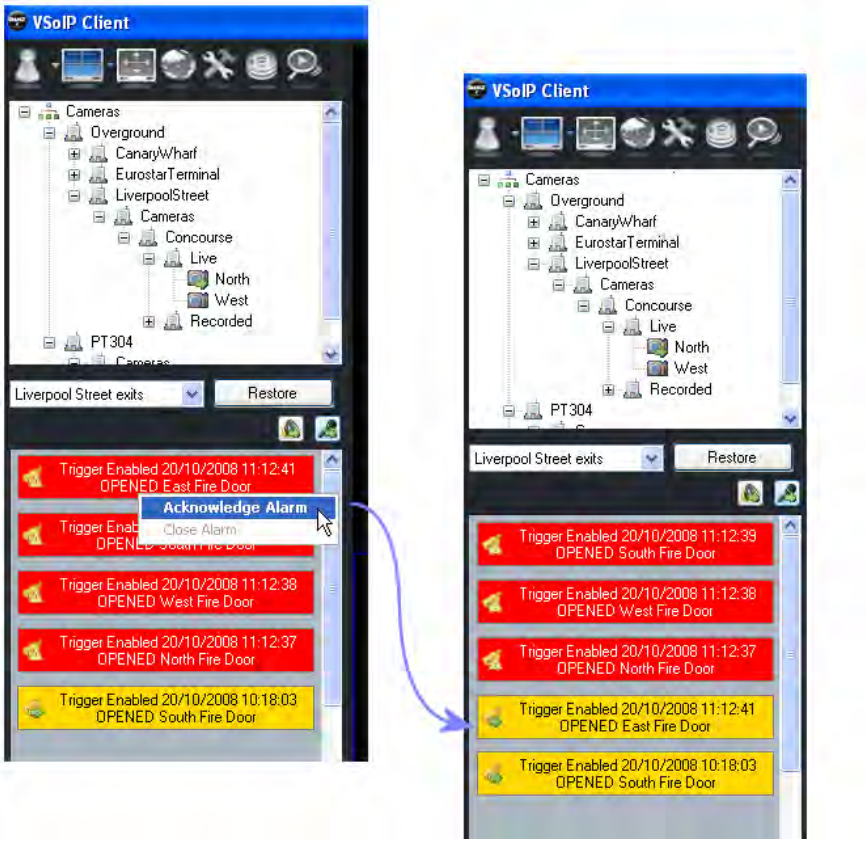


Figure 48 Acknowledging an alarm

1 Right-click alarm you want to acknowledge, then select Acknowledge Alarm. Alternatively, simply left-click the alarm to acknowledge it.

2 The alarm changes to yellow to show it has been acknowledged.

When a user acknowledges an alarm, the server notifies all connected clients, which in turn update the alarm display to reflect the new state of the alarm.

Caution: Please note that if you have chosen to display video from complex alarms on a Video-wall and have also chosen to manually acknowledge alarms, a user must be logged in to VSoIP Pro to do this as it is not possible to manually acknowledge alarms using the Video-wall. See “Displaying Live Video on all Connected Clients and Video-walls” on page 76 for more information.

Automatic Acknowledgement

The client application can automatically acknowledge complex alarms. For information on how to configure this, see “Auto-Acknowledging Alarms” on page 77.

Closing an Alarm

Figure 49 Closing an alarm

Note: When you close an alarm, all clients connected to the server remove the closed alarm from the alarm display (this may take a short time).

Playing Back Recorded Video

VSoIP Pro allows users to view video up to 36 recordings simultaneously, recorded on Networked DVRs and NVRs.

Note: No more than 36 combined live views or playback views may be active at any one time. An error message is displayed if you attempt to view more than this number.

Note: In this section the term *recorders* is used to mean Networked DVRs or NVRs.

Playback functionality is very flexible and permits playback from more than one camera on the same recorder, cameras from different recorders, and the same camera on the same recorder at different times, or some permutation of these.

Note: Be aware of the load placed on various parts of the network and on the devices themselves when requesting playback sessions.

The server manages access to recorders within the surveillance site. To play back video from recorders a user must belong to a group with appropriate privileges to view the IP camera or Networked DVR analogue input AND have permitted access to the recorder.

Discovering Recorded Footage

To view recordings for a device, or set of devices, select an item in the tree.

- If you select a single device, (for example, Elevator in Figure 50), only recordings for that camera are shown.
- If you select a device with more than one camera attached (for example, Covert), or a location which has more than one device associated with it (for example, Underground), all recordings for all devices associated with that item are displayed.
- If more than one recording is shown for a single device, this may be due to an NVR failure during the recording. The recording may have switched automatically from one NVR to another. For more information, please see “NVR Failover” on page 132.
- If the camera associated with a recording is no longer available in the site, the recording is still shown in the list, with the Camera Name shown as “Deleted Device”.

Recordings made by a recorder no longer in the surveillance site are not listed.

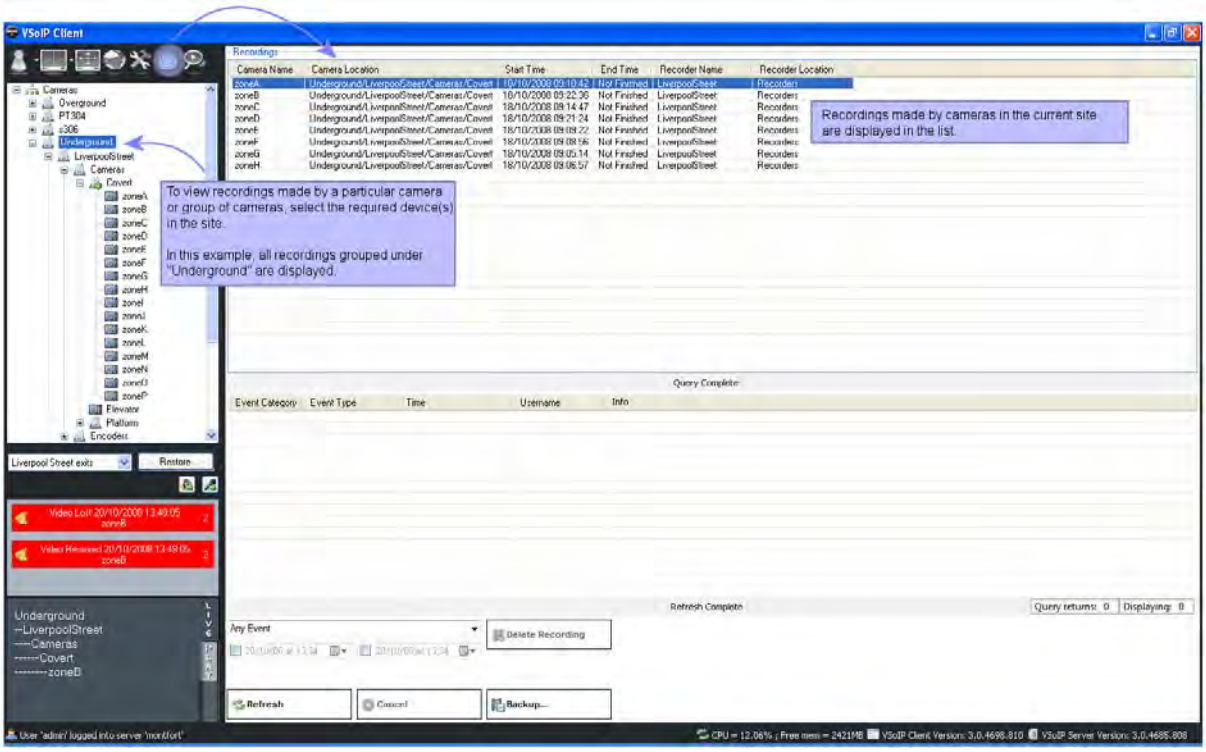


Figure 50 Recordings discovery

Displaying an Events List for a Recording

You may wish to view more information about a particular recording. VSoIP Pro allows you to display all events which occurred while a recording was in progress:

1 Display a list of recordings as described above.

2 Select a recording in the list.

3 Select the type of event you want to display. Select “All events” to display all events which occurred during the recording, including:

- Any complex alarms associated with the device recorded.
- Any complex alarms that may have started an event based recording for this device and the selected recording.

4 In Figure 51, all events which occurred during the recording made by the zoneA camera are displayed.

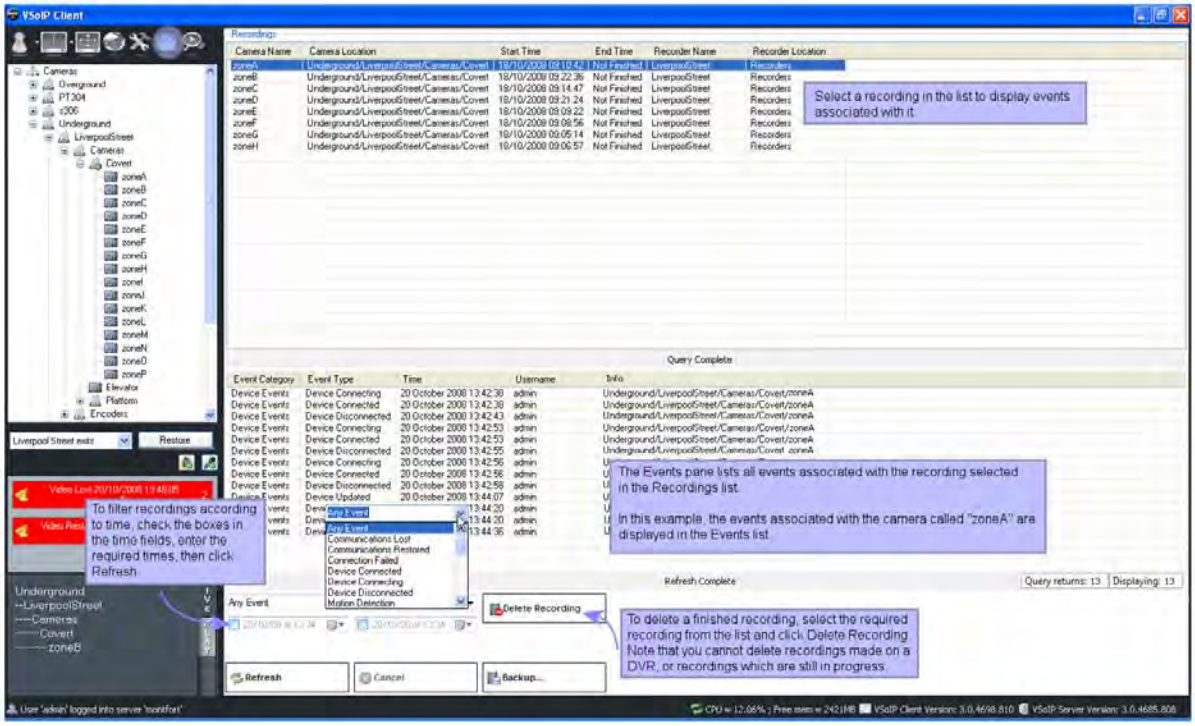

VSoIP Client
Select a recording in the list to display events associated with it.
The Events pane lists all events associated with the recording selected in the Recordings list.
In this example, the events associated with the camera called "zoneA" are displayed in the Events list.
To filter recordings according to time, check the boxes in the time fields, enter the required times, then click Refresh.
To delete a finished recording, select the required recording from the list and click Delete Recording. Note that you cannot delete recordings made on a DVR, or recordings which are still in progress.
Delete Recording
Refresh
Cancel
Backup...

Figure 51 Listing events for a selected recording

5 Double-click any of these events to start playing back the recording from the time of the selected event. The recording is displayed in the top-left corner of the recordings window, which switches automatically to a 2x2 layout.

Playing Back Recorded Footage

To play back recorded footage, follow the steps outlined in Figure 52.

Note: To view a recording on the second monitor of a dual-head setup, drag and drop the camera whose recording you want to view onto a video pane on the second monitor. The playback controls and timeline for that recording are displayed on the main monitor.

VSoIP Client
1. Select Playback view, and the number of video panes you want to display.
Cameras
Overground
Underground
LiverpoolStreet
Cameras
Covert
zoneA
zoneB
zoneC
zoneD
zoneE
zoneF
zoneG
zoneH
2. All cameras from which there are recordings are shown in the site.
3. Drag and drop the camera whose recordings you want to view onto a video pane.
If more than one recording is found from that camera, these are listed.
VSoIP Recorder : 14/08/09 10:39
VSoIP Recorder : 17/08/09 09:23 *
VSoIP Recorder : 17/08/09 13:17 *
4. Select the recording you want to view from the list. The recording starts to play in the chosen pane.
Click once in the pane to activate the recording controls and timeline.
A green square indicates that the watermark on the recording is intact and that the recording has not been tampered with.
If a red squre is displayed, it indicates that the recording may have been tampered with.
Liverpool Street exits
Restore
Trigger Enabled 21/10/2008 08:33:34 OPENED North Fire Door
Video Lost 21/10/2008 08:42:00 zoneB
Video Restored 21/10/2008 08:42:00 zoneB
17/08/2009 13:22:53.831 x 1.00
17/Aug/09 at 09:23:10
Goto...
Synchronise Playback
User 'admin' logged into server 'montfort'
CPU = 4.49

Figure 52 Initial playback and reviewing footage

If your mouse has a scroll button, you can zoom in and out quickly on the timeline. Position your mouse over the area of the timeline you want to view in more detail, and move the scroll button up to zoom in, and down to zoom out.

Note: Some DVRs cannot provide timeline information to VSoIP in intervals smaller than blocks of several minutes. If this is the case, then if there is ANY footage stored by the DVR during that period, no matter how short in duration, VSoIP will show a timeline entry that covers the entire duration of the block despite the actual footage being shorter than the block. This is a limitation of the DVR concerned and not VSoIP.

When this occurs, clicking the timeline causes VSoIP to play the closest available footage immediately prior to the requested footage if no actual footage is available.

Playback Controls

Once playback starts, various playback controls are available: rewind, fast forward, pause, resume, step-forward, step-back. Also, the current position is indicated as a date and time.

Note: Not all recorders can perform every playback control, e.g. step-back. If an operation is not possible, the request to perform it is ignored.

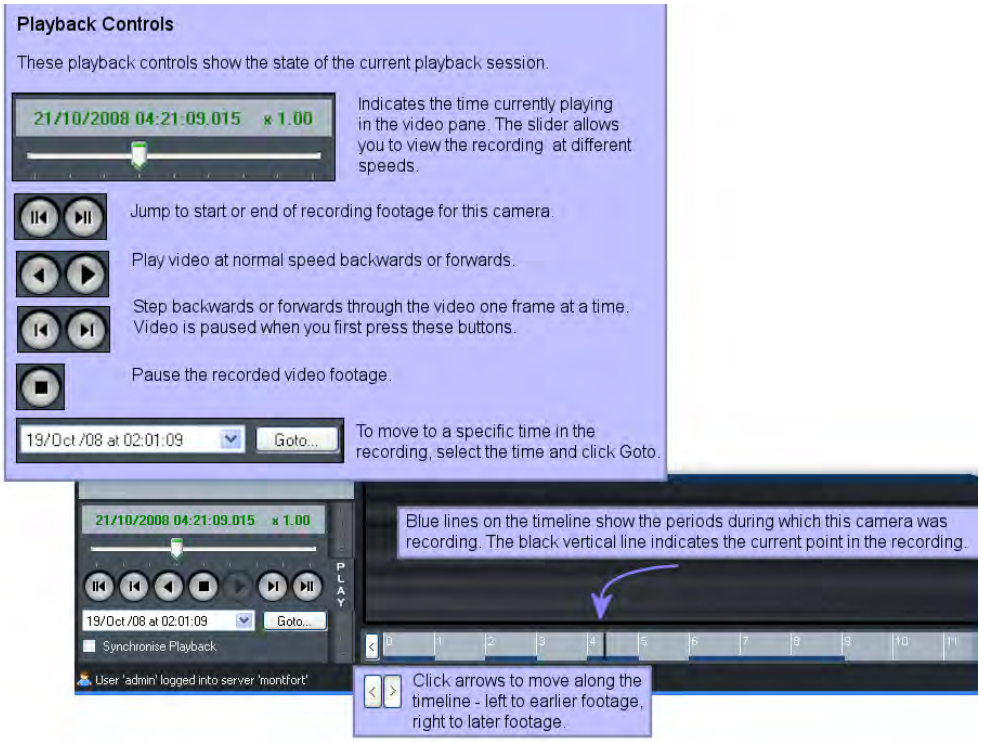

Playback Controls
These playback controls show the state of the current playback session.
21/10/2008 04:21:09.015 x 1.00
Indicates the time currently playing in the video pane. The slider allows you to view the recording at different speeds.
Jump to start or end of recording footage for this camera.
Play video at normal speed backwards or forwards.
Step backwards or forwards through the video one frame at a time. Video is paused when you first press these buttons.
Pause the recorded video footage.
19/Oct /08 at 02:01:09
Goto...
To move to a specific time in the recording, select the time and click Goto.
21/10/2008 04:21:09.015 x 1.00
PLAY
19/Oct /08 at 02:01:09
Goto...
Synchronise Playback
User 'admin' logged into server 'montfort'
Blue lines on the timeline show the periods during which this camera was recording. The black vertical line indicates the current point in the recording.
Click arrows to move along the timeline - left to earlier footage, right to later footage.

Figure 53 Controlling playback

Using Digital Zoom

VSoIP Pro allows you to zoom in on and move around recorded video footage.

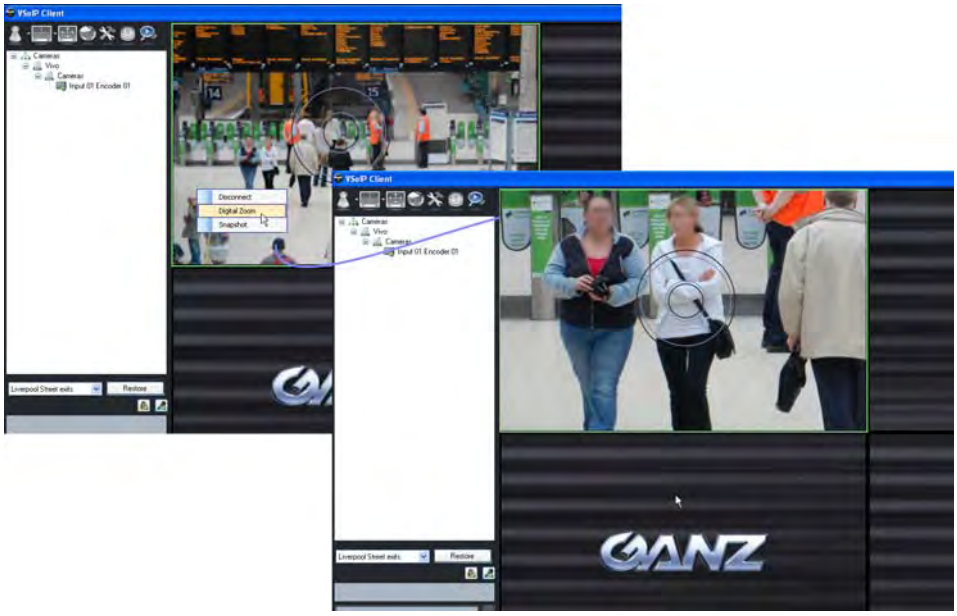


Figure 54 Zooming in to recorded video

Click the part of the video pane that you want to see in more detail, then use the mouse scroll button to zoom in and out as required. While zoomed in, click away from the centre of the image to pan the video.

Taking a Snapshot of Recorded Video

VSoIP Pro allows you to capture snapshots of recorded video playing in a video pane. By default, these are saved to \Desktop\VSoIP Image Clips\FromRecordings, as .jpeg images. To change this location, see “Changing Client Settings” on page 117.

To take a snapshot, right-click in the pane displaying the video at the point you want to capture, and select Snapshot.

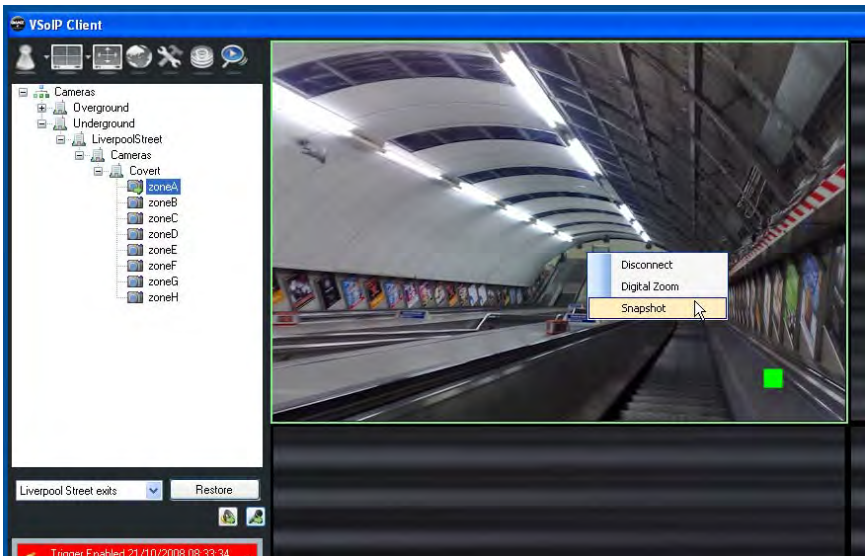


Figure 55 Taking a snapshot of recorded video

Synchronising Playback of Recorded Footage

To help operators review recorded footage from multiple cameras on multiple networked DVRs and/or NVRs simultaneously, it is possible to control playback using a master set of playback controls. This allows playback to be paused and “wound” forward or backwards at the same time saving time switching between playback sessions.

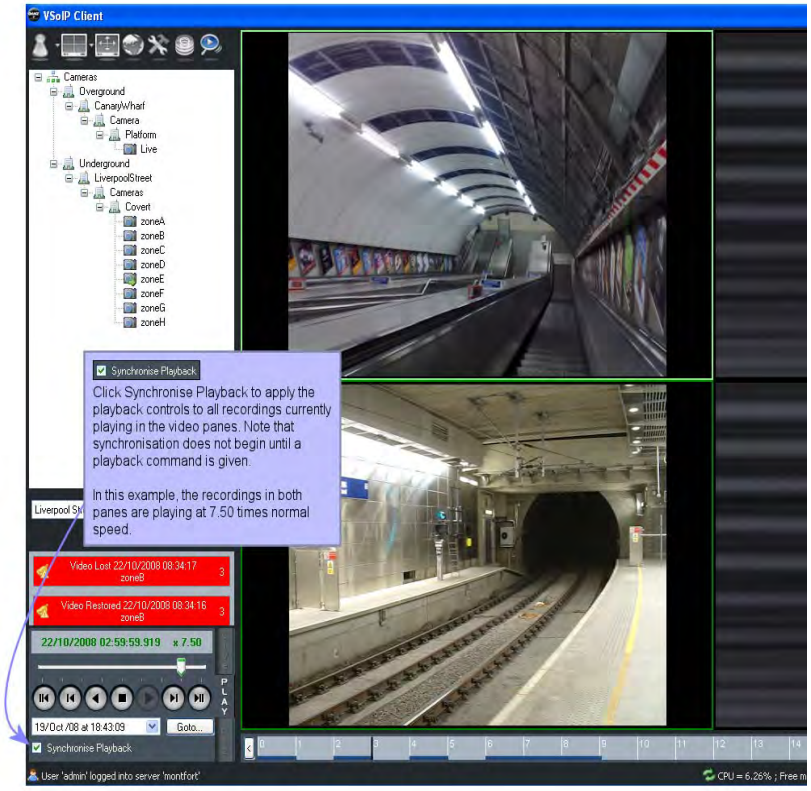


Figure 56 Synchronised playback

Note: Networked DVRs can vary in their performance. Some are limited to a certain number of concurrent playback sessions. The performance of the application during synchronised playback will reflect the responsiveness and performance of the poorest responding and performing element. Note also that after an extended period of synchronised playback, video in some panes may become de-synchronised. Click Pause, then Play to re-synchronise the panes.

Exporting Recorded Video

For evidential purposes, it is often necessary to extract a portion of recorded footage for playback in a player application.This permits recorded footage to be viewed without requiring a client to be connected via a server to a recorder – instead a simpler reproduction system is used, e.g. a standalone laptop.

You can:

- Export an individual recording
- Export several recordings simultaneously.

Note: The procedure for exporting single or multiple recordings is identical, except for the number of recordings you select.

Exporting One or More Recordings

Locate your recording in the list of recordings of IP cameras and camera inputs on Networked DVRs.

Figure 57 shows the steps required to export recording footage.

Note: If you are exporting recordings that have audio associated with them, you can choose to export just the video, or video with audio. Note that audio can only be exported in native mode, not in MP4 format (see “VSoIP Player” on page 71).

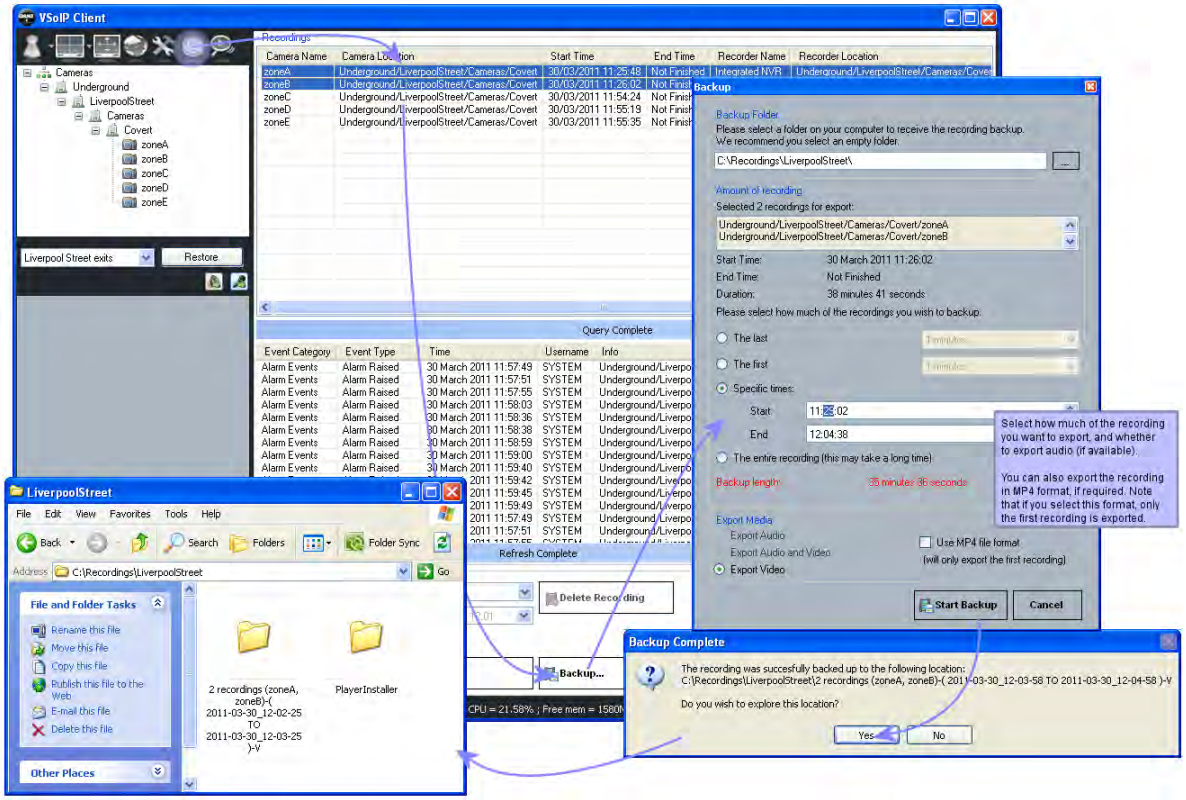


Figure 57 Exporting recording footage

Note: When you select video footage to export, VSoIP Pro checks the integrity of the selected video and informs you if the export is likely to encounter problems.

If you export more than one recording at the same time, the exports are merged into a single .csx file. It is still possible to play each recording separately using the VSoIP Player.

VSoIP Player

VSoIP Player is designed to maintain the evidential integrity of the original recording by keeping the recording in its native format. Unlike other forms of export, e.g. MP4, native exporting means that the exported recording has not been transcoded or altered in any way.

When the client is instructed to export recordings in native format, it copies the VSoIP MultiPlayer Installer at the same time. This contains two Player applications:

- VSoIP Player — Used to to play back recordings exported from a client application. It can play multi-camera recordings (.csx), and legacy recordings (.cve and .cvc).
- VSoIP Web Player — Primarily used to play media streams originating from RTSP-based sources, such as a transcoder/broadcaster. It can also be used to play back legacy recordings in .cve and .cvc format.

This create an evidence “package” for use by individuals without access to the clients, server and the Networked DVRs and NVRs of the surveillance system — one folder contains a single file with the exported recording(s), the other contains the Player installer.

Note: Although the computer running VSoIP Player can be considered to be a general purpose PC, it must support Microsoft Direct-X 3D rendering to a reasonable performance level.

For information on using VSoIP Player, please see the VSoIP Player User Guide.

Audit Trail Configuration

The audit trail provides a comprehensive list of events that have occurred since the server component was installed. Some examples of event information are:

- Alarms (acknowledgement, closed).
- Users (added, deleted, edited etc.).
- Devices (added, updated, deleted, disconnected etc.).
- Recording (disk space low or critical).

This list is not comprehensive – many other types of event are also monitored.

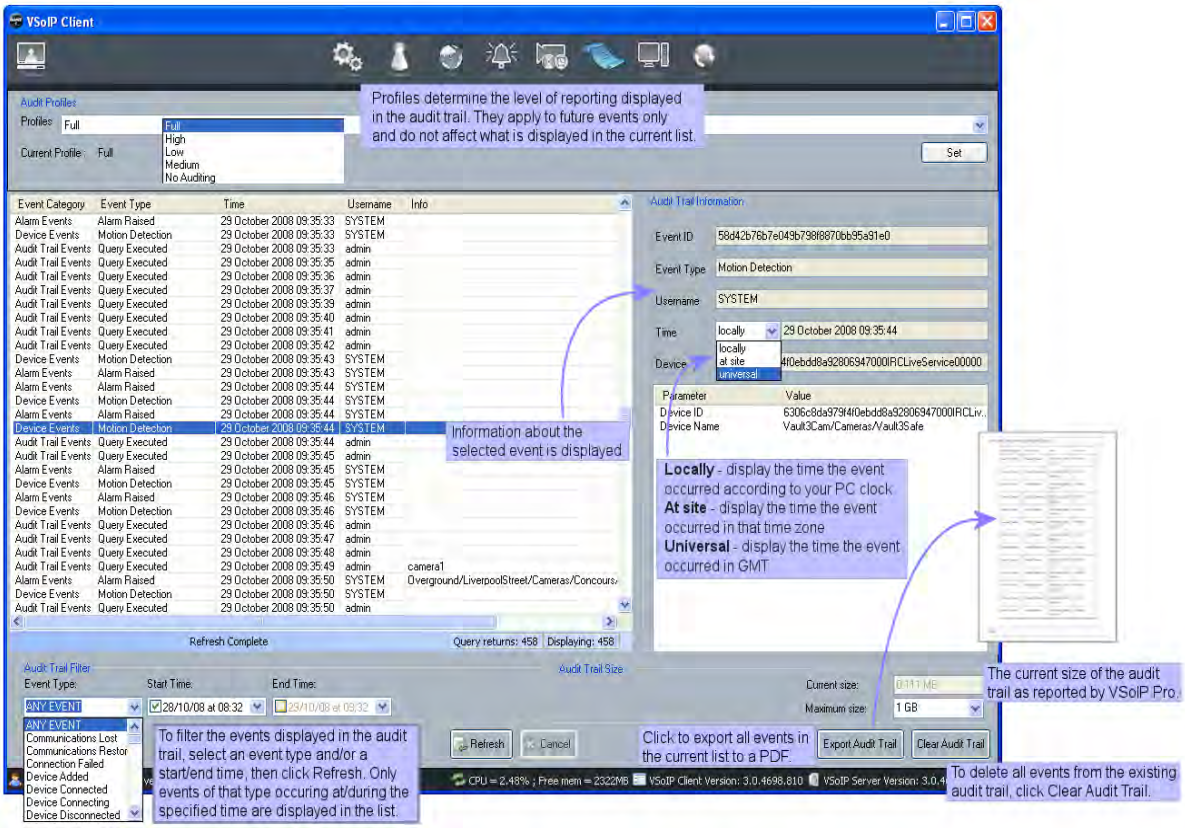

VSoIP Client
Profiles determine the level of reporting displayed in the audit trail. They apply to future events only and do not affect what is displayed in the current list.
Information about the selected event is displayed
Locally - display the time the event occurred according to your PC clock
At site - display the time the event occurred in that time zone
Universal - display the time the event occurred in GMT
The current size of the audit trail as reported by VSoIP Pro
To filter the events displayed in the audit trail, select an event type and/or a start/end time, then click Refresh. Only events of that type occuring at/during the specified time are displayed in the list.
Click to export all events in the current list to a PDF
To delete all events from the existing audit trail, click Clear Audit Trail.

Figure 58 The audit trail

Caution: When specifying the maximum size for the audit trail, please be aware of the following:

If you have installed the NVR on the same PC as the VSoIP Pro Server, meta-data associated with recordings is also stored in the SQL database, as well as audit trail data. The maximum total space used in the database for audit trail and recording meta-data cannot exceed 4GB. Please consider this when setting the size of the audit trail database.

Audit Trail Profiles

By default, the audit trail lists all events that have occurred since server installation, or since the audit trail was last cleared. Some of these events may be of more interest to you than others. *Profiles* allow you to specify which events you want to display in the audit trail.

There are five audit trail profiles — full, high, low, medium and No Auditing. The default settings are as follows:

Table 7 Default Audit Trail settings

Low	• Server Started • Server Shutdown • Service Hosted • Service Shutdown • User Login • User Logout • Security Failure • Session Timeout	• Alarm Raised • Alarm Acknowledged • Alarm Closed • Alarms To Raise Changed • Device Connected • Device Disconnected • Video Lost • Video Restored
Medium - all of the above, plus:	• User Added • User Deleted • Group Added • Group Deleted	• Device Added • Device Removed • Mapset Added • Mapset Deleted
High - all of the above, plus:	• Group Members Changed • Group Updated • User Updated	• Connection Failed • Device Connecting • Mapset Updated
Full - all of the above, plus:	• Communications Lost • Communications Restored • Device Updated • Motion Detection • Stream Lost • Trigger Alarm • Lease Lost • Current Profile Changed • Profile Added • Profile Removed • Profile Updated • Query Executed • Audit Trail Cleared • Mapset Added • Mapset Deleted • Mapset Updated • Recording Created	• Recording Deleted • Recording Finished • Recording Source Closed • Recording Start Changed • Recording Started • Recording Stopped • Recording Tagged • Disk Space Critical • Disk Space Low • Job Created • Job Finished • Job Started • Play Closed • Play Created • Play Started • Play Stopped

Audit Trail Management

VSoIP Pro automatically reduces the size of the audit trail once it becomes full, however it is preferable to carry out regular audit trail management to prevent the audit trail from reaching maximum capacity.

The audit trail is stored as a table in an SQL database. The system administrator can manually reduce the size of the database table by deleting entries that are no longer required, or by backing up the table and deleting it.

To locate the table:

1 Open your SQL application.

2 In the main window, double click Databases>VSoIPSuite3>Tables to locate the VSoIP audit tables. From here, you can back up the tables and perform other maintenance operations. Please refer to the SQL Server documentation for more information.

Automatic Deletion

When the database table reaches 90% of its possible capacity, VSoIP Pro displays a popup to indicate that the table is nearly full.

Additional popups are displayed every time another 1% of the audit trail is used. If no manual action is taken to reduce the table size, once the table becomes full, VSoIP Pro automatically reduces the table size to the smaller of the following two options:

- Entries for the last 7 days.
- The most recent 10% of entries

Note: During the reduction process, users have read-only access to the system.

Caution: If audit trail data needs to be stored long-term, the system administrator should carry out a backup operation on a regular basis.

Chapter 6 – Complex Alarm Configuration

This chapter contains the following information:

- Simple, Scheduled and Device-specific Alarms
- Complex Alarm Actions
- Creating Complex Alarms
- Using the NOT Boolean Operator
- How Complex Alarms Work
- Example of Complex Alarm Processing

Simple, Scheduled and Device-specific Alarms

Complex alarms are created by combining simple alarms and time schedules together to form more complex alarm processing logic. This section considers creating complex alarms from simple alarms and time schedules.

Simple Alarms

A simple alarm represents an alarm source on an IP Camera, encoder or Networked DVR within the surveillance system.Examples of such alarm sources are:

- Binary inputs (eg, closing contacts).
- Motion detector alarms.
- Video loss alarms.
- Networked DVR complex alarm logic, resulting in an alarm on the DVR.

Scheduled Alarms

A schedule is another type of alarm source. A server can be the source of one or more alarms based on a schedule. A schedule is a time-based alarm source that causes an alarm to be continuously output when the time and day of a week matches a marked period within the schedule. Each marked period represents one hour. Each schedule has seven days of twenty-four hour long periods available. Any number of periods can be chosen.

Examples of schedules an administrator level user might create on a server are:

- All weekend — all periods for Saturday and Sunday are selected.
- Outside weekday office hours — Monday to Friday, periods representing hour long intervals after 1800h until interval prior to 0900h, are selected.
- During lunch-hour — A period of one hour after 12h00 for each weekday is selected.

Device-Specific Alarms

Certain device-specific alarms are supported, for example, analytics alarms. These alarms can be used as inputs to complex alarms. Please see the device specific application notes for more information on these alarms.

Complex Alarm Actions

When creating a complex alarm, it is possible to specify that one or more of the following actions should take place when the alarm is triggered:

- Live video should be displayed on all connected clients and Video-walls.
- Complex alarms should be auto-acknowledged by the server.
- A relay action should be activated.

These are further explained below.

Displaying Live Video on all Connected Clients and Video-walls

Note: Users logged into the remote client(s) on which video is to be displayed must belong to a user group for which Alarm Actions is enabled. See “Creating a User Group” on page 36 for details on how to do this.

To specify that live video should be displayed on remote clients and Video-walls when an alarm occurs:

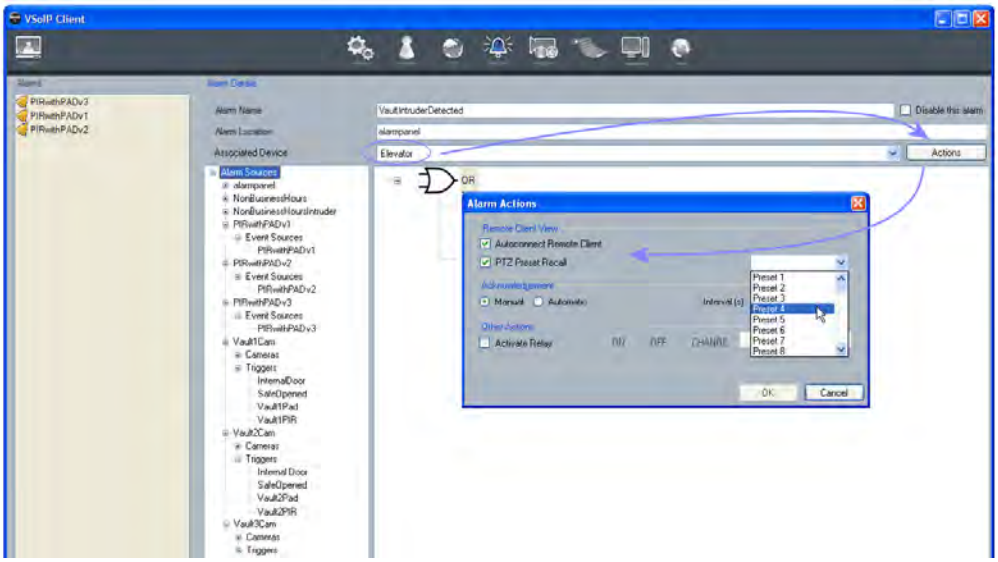


Figure 59 Specifying the remote client alarm action

1 Click to enter complex alarm configuration mode.

2 Click Add.

3 Enter a name for the alarm and (optionally) a location.

4 Select the device or sequence that you want to associate with this complex alarm.

5 Click Actions to display the Alarm Actions dialog.

6 Select “Autoconnect Remote Client”.

7 If the device you have associated with this alarm has PTZ capability, select PTZ Preset Recall and select the preset that you want to be displayed, if required.

Note: If you are associating sequences which use PTZ presets with alarm actions, please be aware that there may be a conflict between the sequence preset and other complex action PTZ preset requests.

8 Click OK.

9 Create the required alarm logic (see “Creating Complex Alarms”, below), and click OK.

When the alarm occurs, remote clients auto-connect to the live video source. For details on how to specify where the alarm video appears on the remote client, see:

- “Viewing System Information” on page 114 for remote clients.
- The configuration chapter of the VSoIP Video-wall or VSoIP Display User Guide.

Auto-Acknowledging Alarms

To specify that complex alarms should be automatically acknowledged after a set period:

1 Click Add.

2 Enter a name for the alarm and (optionally) a location.

3 Select a device or sequence that you want to associate with this complex alarm (optional).

4 Click Actions to display the Alarm Actions dialog.

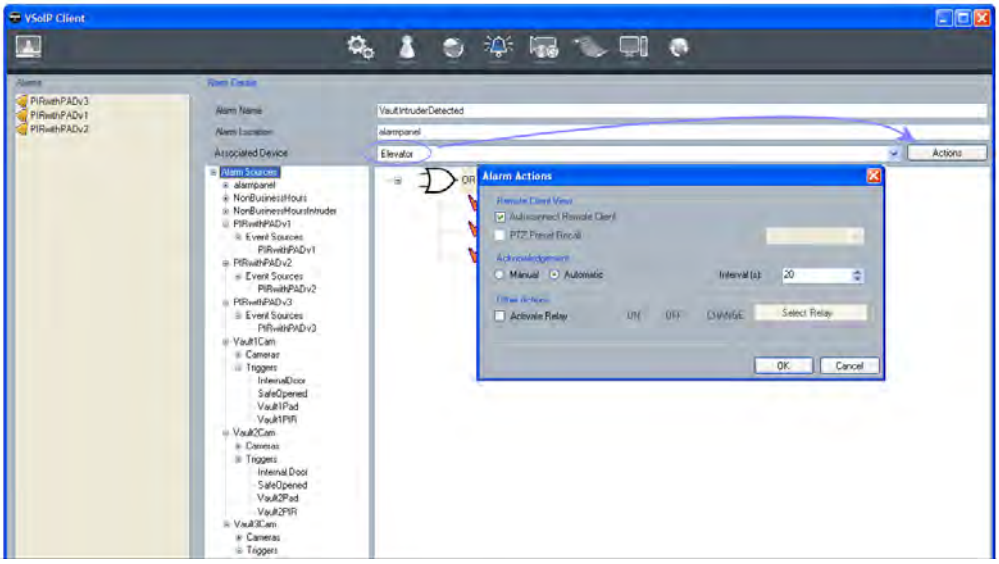


Figure 60 Specifying auto-acknowledgement for complex alarms

5 Select Automatic, and specify after how many seconds the alarm should be automatically acknowledged. The default value is 20 seconds.

Note: Only complex alarms can be auto-acknowledged. Simple alarms must be manually acknowledged by the user.

Caution: Please note that if you have chosen to display video from complex alarms on a Video-wall and have also chosen to manually acknowledge alarms, a user must be logged in to VSoIP Pro to do this as it is not possible to manually acknowledge alarms using the Video-wall.

Activating a Relay on an Alarm

To activate a relay when a complex alarm occurs:

1 Click Add.

2 Enter a name for the alarm and (optionally) a location.

3 Select the device that you want to associate with this complex alarm (optional).

4 Click Actions to display the Alarm Actions dialog.

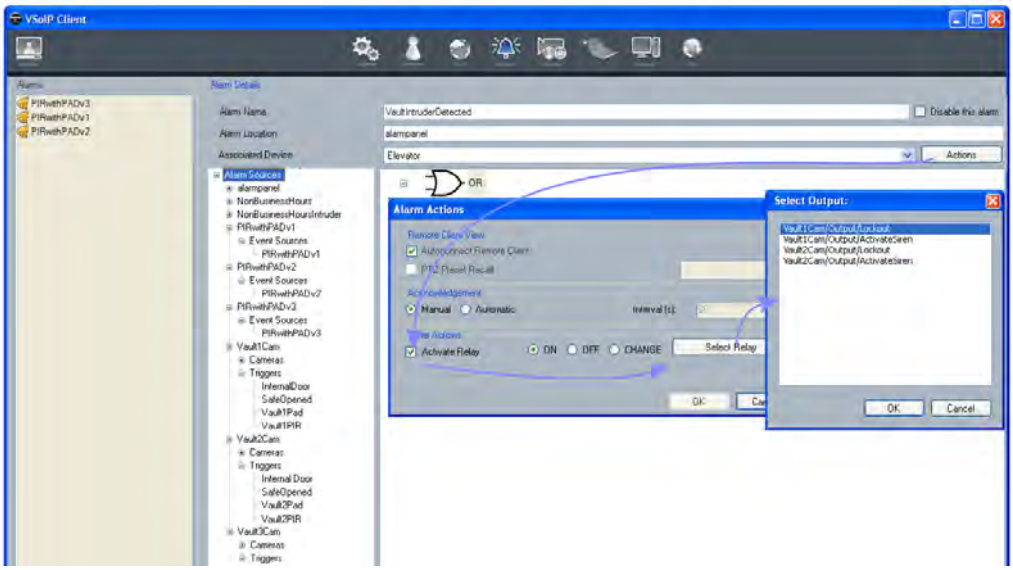


Figure 61 Specifying relay activation for complex alarms

5 Check Activate Relay, then click Select Relay.

Note: If Activate Relay is unavailable, check that you have selected a device and not a sequence in the Associated Device field. Sequences are not supported here.

6 Select the required relay from the list and click OK. When this alarm is triggered, the relay is activated.

Note: Click Change to toggle the relay on or off, for example, to turn on a light if it is currently off, and vice versa.

Understanding Alarm Processing

A common technique used to represent logic expressions like those described previously is a logic system called Boolean logic. The inputs and outputs of Boolean logic expressions are either true or false. These states can be thought of as voltages present (TRUE) or absent (FALSE) at an input and voltages present (TRUE) or absent (FALSE) at an output.

In Boolean logic a condition represents something which takes one or more inputs and produces a single output which is either true or false depending on the states of the input(s) and the Boolean logic condition being used. Examples of Boolean logic are explained in the following section.

Creating Complex Alarms

To illustrate the creation of complex alarms, we shall use the following scenario.

A surveillance system has equipment monitoring three bank vaults using PIR sensors connected to IP cameras and pressure pads connected to a Networked DVR.

The aim of the system's designer is to have an alarm triggered when all of the following conditions apply:

- a PIR AND a pressure pad are activated
- in ANY of three bank vaults
- during non-business hours

Note: It is also possible to achieve the same end result by setting up a single complex alarm. However, a modular structure is useful because it allows individual elements to be altered separately, and reused within other complex alarms.

Note: Only administrators can create, modify and delete alarms and their actions.

Step 1

To prevent false alarms, the system's designer has specified that a vault's intruder alarm should *only* be triggered when the pressure pad AND the PIR trigger in that vault are both activated, i.e. both sensors change state from FALSE to TRUE.

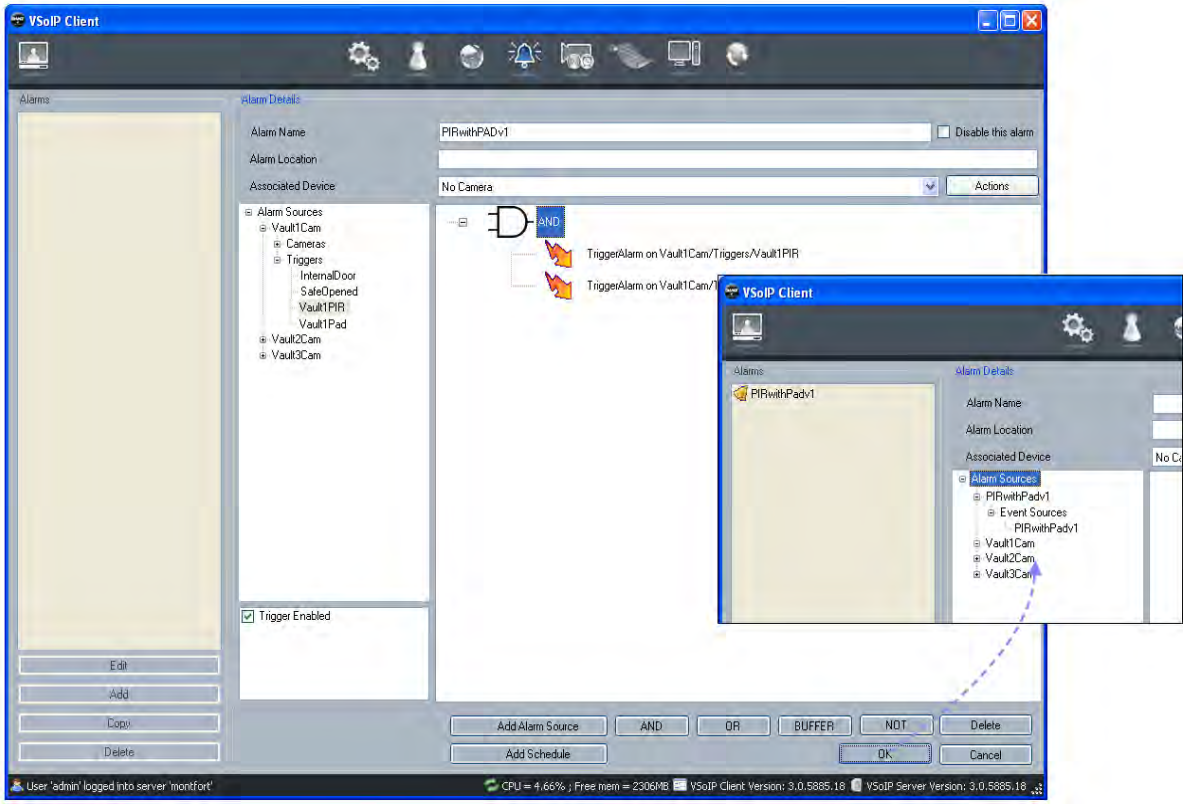


Figure 62 Creating PIRwithPADv1 complex alarm

1 Click to enter complex alarm configuration mode.

2 Click Add.

3 Enter a name for the alarm and (optionally) a location. In this example, the alarm is called PIRwithPADv1.

4 Click the Boolean logic operator button required for the part of the alarm logic you are describing; in this example it is AND (i.e. /Vault1Cam/Triggers/Vault1PIR AND Vault1Cam/Triggers/Vault1Pad). The symbol for this operation appears in the alarm logic designer pane.

Note: AND is the logic condition for “all inputs must be active”. All inputs of an AND logic expression must be TRUE for the output to be TRUE.

5 Select the alarm source you want to use from the list. The events that that alarm source can generate are listed. Put a check against the event that should cause an alarm from the alarm source.

Note: If, for example, a video-based alarm source had been chosen, other possible events could have been checked such as video loss or video motion detected.

6 Click Add Alarm Source.

7 Repeat steps 4 and 5 until the required logic is achieved. In this example, Vault1PIR is added in the same way.

8 When finished, click OK. The output of this conditional expression becomes a new complex alarm, e.g. /PIRwithPADv1. When the /Vault1Cam/Triggers/Vault1PIR sensor and /Vault1Cam/Triggers/Vault1Pad sensor are both activated, then the /PIRwithPADv1 complex alarm will fire.

9 In this example, steps 1-7 would be repeated for vaults 2 and 3.

Note: If you make a mistake, select the item and click Delete. We recommend that you write out your logic design on paper first, then place *only* the logic operators on the pane, then finally add in the alarm sources and schedules.

Step 2

The system’s designer has specified that a secondary alarm must be triggered if ANY ONE of the vaults is breached, i.e. when any one of the vaults’ PIRwithPAD trigger changes state from FALSE to TRUE.

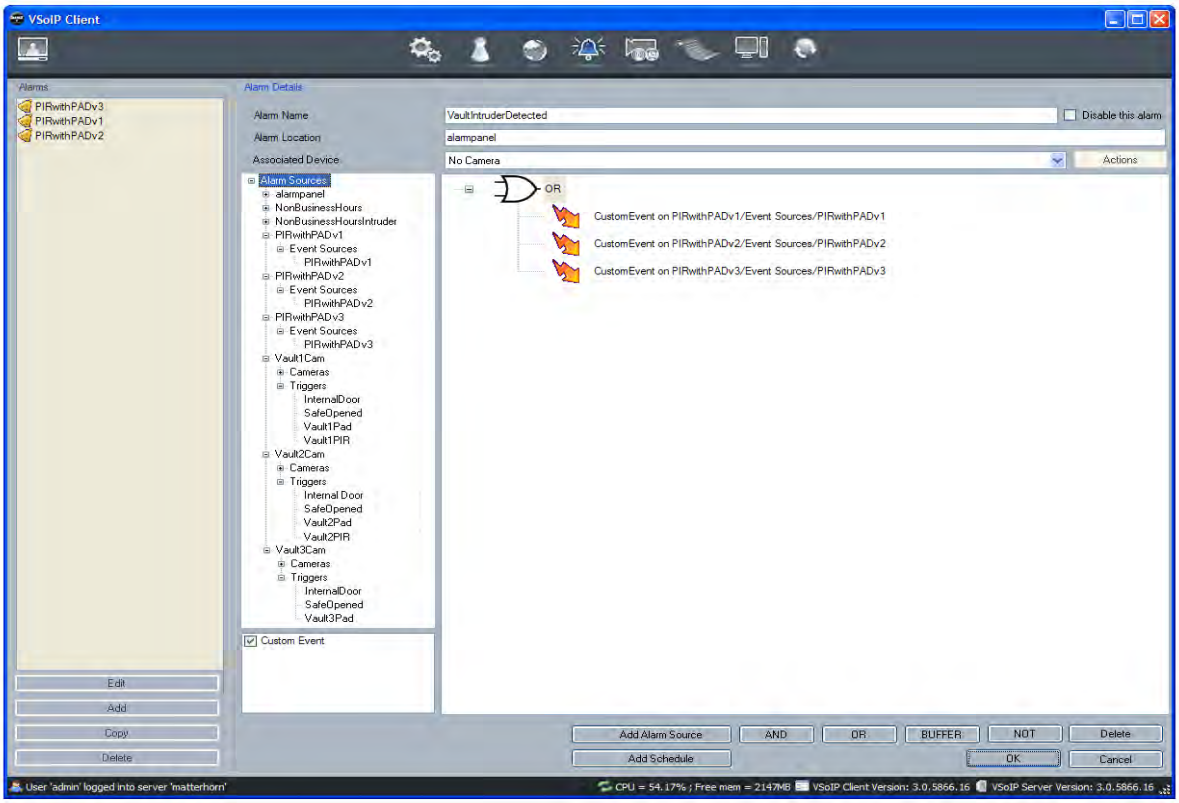


Figure 63 Creating VaultIntruderDetected complex alarm

1 Click Add.

2 Enter a name for the alarm and (optionally) a location. In this example, the alarm is called VaultIntruderDetected and the location is alarmpanel.

3 Click the Boolean logic operator button required for the part of the alarm logic you are describing; in this example it is OR (e.g. /PIRwithPADv1 OR /PIRwithPADv2 OR /PIRwithPADv3). The symbol for this operation appears in the alarm logic designer pane.

Note: OR is the logic condition for “any inputs are active”. If ANY inputs of an OR logic expression are TRUE then the output will be TRUE.

4 Select the alarm source you want to use from the list, remembering to choose an event available from the source, and click Add Alarm Source. In this case, the alarm source PIRwithPADv1 is the first to be added.

5 Repeat step 4 until the required logic is achieved. In this example, PIRwithPADv2 and PIRwithPADv3 are added in the same way.

6 When finished, click OK. The output of this conditional expression becomes a new complex alarm, e.g. /alarmpanel/VaultIntruderDetected. When the /PIRwithPADv1 or /PIRwithPADv2 or /PIRwithPADv3 is activated then the /alarmpanel/VaultIntruderDetected complex alarm is triggered.

Step 3

The third alarm that the designer must create is a scheduled alarm. This is a time-based alarm source that causes an alarm to be continuously output when the time and day of a week matches a marked period within the schedule.

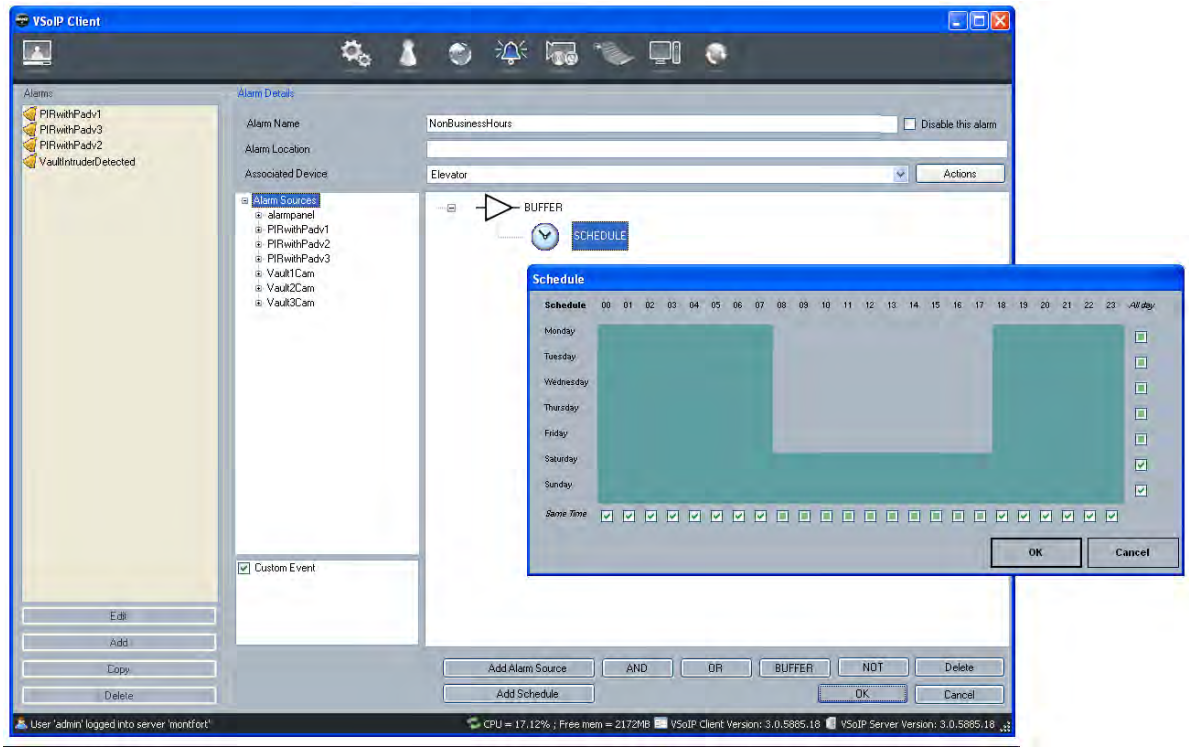


Figure 64 Creating NonBusinessHours scheduled alarm

1 Click Add.

2 Enter a name for the alarm and (optionally) a location. In this example, the alarm is called NonBusinessHours.

3 If required, select the device associated with this complex alarm.When the alarm occurs, you can then drag and drop the alarm into a video pane to view live video from that camera. VSoIP Pro can carry out several actions when a complex alarm occurs. For further information, please see “Complex Alarm Actions” on page 76.

4 Click the Boolean logic operator button required for the part of the alarm logic you are describing, or, if the schedule does not need to be part of a more complex alarm logic system, click BUFFER.

5 Click Schedule. In the Schedule dialog, select the hours you want the alarm to be continuously output. In this example, the schedule is active from 18:00 every evening until 08:00 the following morning, and at weekends. Check the box for a row/column to select the entire row/column.

Note: To edit an existing schedule, right-click the clock icon and select Edit Schedule.

6 Click OK when finished.

Step 4

Finally, the designer needs to create a complex alarm that combines the alarms he has set up already. This complex alarm would be triggered when a PIR AND a pressure pad are activated in ANY of the three vaults during non-business hours.

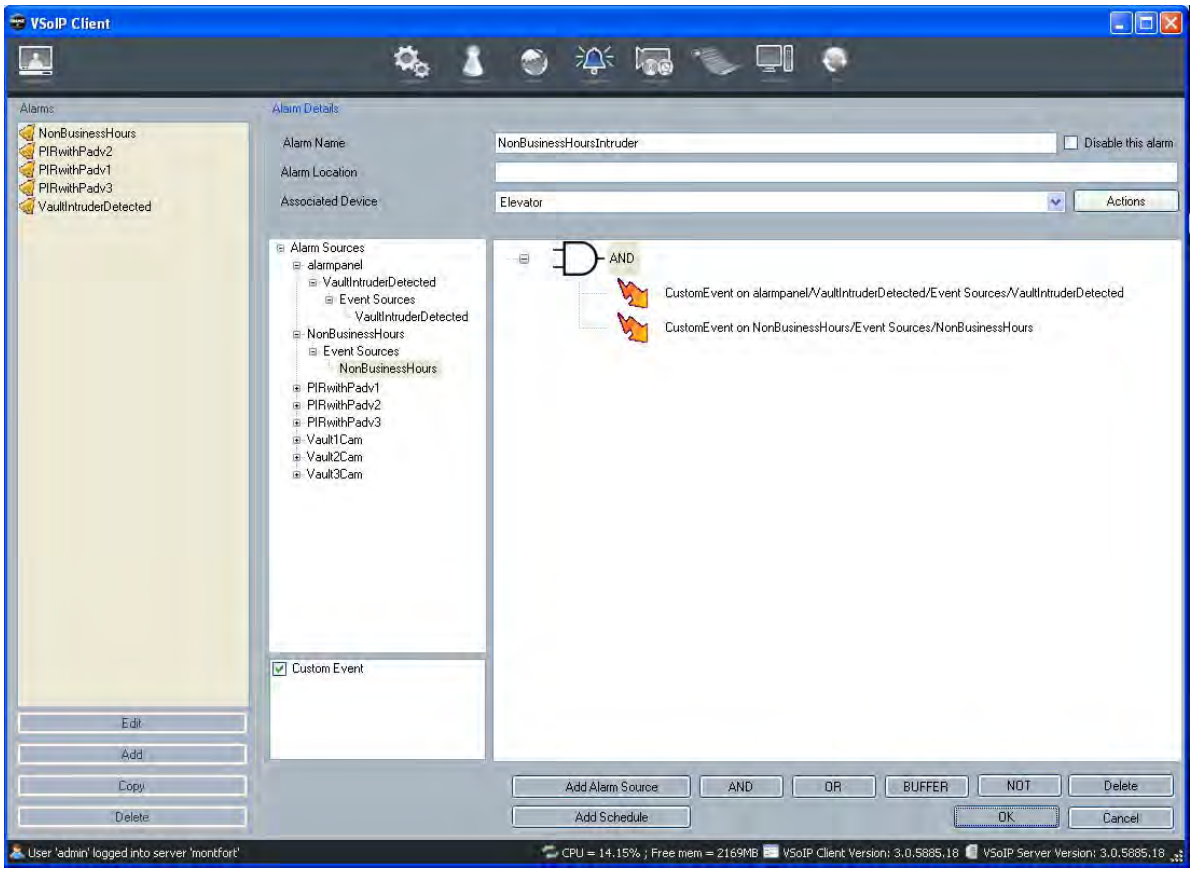


Figure 65 Creating NonBusinessHoursIntruder Complex Alarm

1 Click Add.

2 Enter a name for the alarm and (optionally) a location. In this example, the alarm is called NonBusinessHoursIntruder.

3 If required, select the device associated with this complex alarm. When the alarm occurs, you can then drag and drop the alarm into a video pane to view live video from that camera.

VSoIP Pro can carry out several actions when a complex alarm occurs. For further information, please see “Complex Alarm Actions” on page 76.

4 Click the Boolean logic operator button required for the part of the alarm logic you are describing; in this example it is AND (e.g. /alarmpanel/VaultIntruderDetected AND /NonBusinessHours). The symbol for this operation appears in the alarm logic designer pane.

Note: AND is the logic condition for “all inputs must be active”. All inputs of an AND logic expression must be TRUE for the output to be TRUE.

5 Select the alarm source you want to use from the list, remembering to choose an event available from the source, and click Add Alarm Source. In this case, the alarm sources /alarmpanel/VaultIntruderDetected and /NonBusinessHours are added.

6 When finished, click OK. The output of this conditional expression becomes a new complex alarm, e.g. /NonBusinessHoursIntruder. When the /alarmpanel/VaultIntruderDetected complex alarm is firing and /NonBusinessHours complex alarm is active then the /NonBusinessHoursIntruder alarm will be triggered.

Copying a Complex Alarm

Once you have created a complex alarm, you can use it as a starting point for other alarms, as follows:

1 Click to enter complex alarm configuration mode.

2 Select the alarm you want to copy from the list of alarms, and click Copy.

3 A new alarm is created and displayed in the Alarm Details pane. Its details are identical to that of the alarm you copied, apart from the name, which is “Copy of <alarm name>”.

4 Rename the alarm as required, and make any desired changes, then click OK.

5 The new alarms appears in the alarm list on the left.

Enabling/disabling a Complex Alarm

Sometimes it may be necessary to temporarily disable an individual complex alarm, for example, for maintenance purposes. To disable a complex alarm:

1 Click to enter complex alarm configuration mode.

2 Select the alarm you want to disable from the list of alarms, and click Edit.

3 Select Disable this alarm, and click OK.

Using the NOT Boolean Operator

The above examples made use of the AND and OR Boolean operators and buffers. Another operator, NOT, could be used in conjunction with the NonBusinessHours alarm detailed above, as part of a complex alarm that operates *only during business hours*. Figure 66 illustrates how using NOT reverses the hours during which the alarm is active.

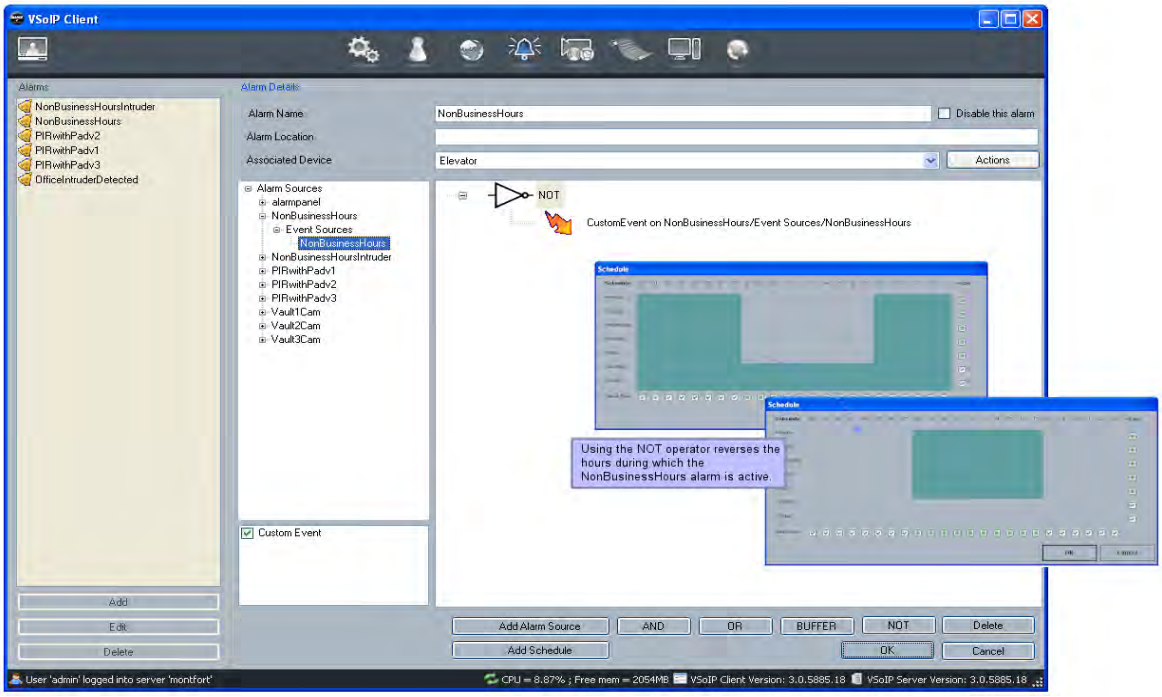


Figure 66 Creating BusinessHours scheduled alarm using NOT Boolean operator

1 Click Add.

2 Enter a name for the alarm and (optionally) a location. In this example, the alarm is called BusinessHours.

3 Click the Boolean logic operator button required for the part of the alarm logic you are describing; in this example it is NOT. The symbol for this operation appears in the alarm logic designer pane.

Note: The Boolean NOT condition outputs TRUE whenever a FALSE is input, or outputs FALSE whenever a TRUE is input.

4 Select the alarm source you want to use from the list, remembering to choose one, or more of the events available from the source, and click Add Alarm Source. In this case, the alarm source /NonBusinessHours is added.

5 When finished, click OK.

How Complex Alarms Work

The server is responsible for keeping track of the state of all simple alarms, scheduled alarms and complex alarms that are included within the logic of each complex alarm.

Whenever an alarm is triggered, the server marks this by changing the alarm's recorded state from FALSE to the TRUE state. The server then maintains this alarm's state as being TRUE for a period of five seconds irrespective of the actual external state of the alarm. After five seconds have elapsed, the server automatically marks the simple alarm as FALSE.

Whenever the server changes the state of an alarm's marked state, the server locates all complex alarms that rely on that alarm and processes the trigger logic. For each alarm included in a complex alarm, the server looks up the last recorded state of the alarm and uses the recorded TRUE or FALSE value in the Boolean logic.

Note: When a complex alarm is evaluated by the server as being TRUE, it is marked as true for a period long enough to evaluate any other complex alarms that refer to it.

Scheduled alarms remain TRUE for as long as the marked period matches the time and day of the week.

The momentary storage of the state (TRUE or FALSE) of the ***output*** of a simple alarm, scheduled alarm or complex alarm for five seconds is automatic and is performed by the server alarm trigger logic processor.

Caution: For a scheduled alarm to be used outside of the alarm processor, a scheduled alarm must be converted to a complex alarm. This is done whenever schedules are a part of the alarm logic for a multi-source complex alarm. If the output required is to be based solely on single scheduled alarm, a complex alarm containing a buffer logic processing element must be used along with the scheduled alarm.

Example of Complex Alarm Processing

The following example details how the server deals with the following scenario: an intruder enters vault one and is detected first by the PIR and then a half a second later they stand on the pressure pad, activating it.

Note: The alarm schedule discussed in Step 3 above is not included in Table 8.

Table 8 Complex alarm walkthrough

Stage	Elasped (msecs)	Activity
PIR detects intruder	T+0000	Simple alarm /Vault1Cam/Triggers/Vault1PIR is received by the server.
	T+0010	The server checks to see if /Vault1Cam/Triggers/Vault1PIR participates in any complex alarms, finds one, and changes the recorded state of /Vault1Cam/Triggers/Vault1PIR from FALSE to TRUE
	T+0176	The server now evaluates all complex alarms containing /Vault1Cam/Triggers/Vault1PIR and finds /PIRwithPADv1. This is a Boolean Logic AND expression between the recorded state of simple alarm /Vault1Cam/Triggers/Vault1PIR and the recorded state of simple alarm /Vault1Cam/Triggers/Vault1Pad. This simplifies to the Boolean condition TRUE AND FALSE which results in FALSE. The complex alarm /PIRwithPADv1 is marked as FALSE.
	T+0193	The server now evaluates all complex alarms containing /PIRwithPADv1 and finds /alarmpanel/VaultIntruderDetected. This is a Boolean Logic OR expression between the recorded states of /PIRwithPADv1, /PIRwithPADv2 and /PIRwithPADv3. Since all of these complex alarms have a recorded state of FALSE, then this simplifies to the Boolean condition FALSE OR FALSE OR FALSE which results in FALSE. Complex alarm /alarmpanel/VaultIntruderDetected is marked as FALSE
	T+0213	The server now evaluates all complex alarms containing /alarmpanel/VaultIntruderDetected and does not find any. Server now considers processing complete.
Pressure pad activated	T+0500	Simple alarm /Vault1Cam/Triggers/Vault1Pad is received by the server.
	T+0508	The server checks to see if /Vault1Cam/Triggers/Vault1Pad participates in any complex alarms, finds one, and changes the recorded state of /Vault1Cam/Triggers/Vault1Pad from FALSE to TRUE
	T+0603	The server now evaluates all complex alarms containing /Vault1Cam/Triggers/Vault1Pad and finds /PIRwithPADv1. This is a Boolean Logic AND expression between the recorded state of simple alarm /Vault1Cam/Triggers/Vault1PIR and the recorded state of simple alarm /Vault1Cam/Triggers/Vault1Pad. This simplifies to TRUE AND TRUE which results in TRUE. The complex alarm /PIRwithPADv1 is marked as TRUE.
	T+0622	The server fires /PIRwithPADv1 alarm.
	T+0629	The server now evaluates all complex alarms containing /PIRwithPADv1 and finds /alarmpanel/VaultIntruderDetected. This is a Boolean Logic OR expression between the recorded states of /PIRwithPADv1, /PIRwithPADv2 and /PIRwithPADv3. These complex alarms now have a recorded state of TRUE, FALSE and FALSE respectively. This simplifies to TRUE OR FALSE OR FALSE which results in TRUE. The complex alarm /alarmpanel/VaultIntruderDetected is marked as TRUE.
	T+0645	The server fires /alarmpanel/VaultIntruderDetected alarm.
		The server now evaluates all complex alarms containing /alarmpanel/VaultIntruderDetected and does not find any. It now considers processing complete.
System clears PIR trigger	T+5010	The server changes the recorded state of /Vault1Cam/Triggers/Vault1PIR from TRUE to FALSE
	T+5098	The server now evaluates all complex alarms containing /Vault1Cam/Triggers/Vault1PIR and finds /PIRwithPADv1. This is a Boolean Logic AND expression between the recorded state of simple alarm /Vault1Cam/Triggers/Vault1PIR and the recorded state of simple alarm /Vault1Cam/Triggers/Vault1Pad. This simplifies to FALSE AND TRUE which results in FALSE. The complex alarm /PIRwithPADv1 is marked as FALSE.
	T+5109	The server now evaluates all complex alarms containing /PIRwithPADv1 and finds /alarmpanel/VaultIntruderDetected. This is a Boolean Logic OR expression between the recorded states of /PIRwithPADv1, /PIRwithPADv2 and /PIRwithPADv3. Since all of these complex alarms have a recorded state of FALSE, then this simplifies to FALSE OR FALSE or FALSE which results in FALSE. The complex alarm /alarmpanel/VaultIntruderDetected is marked as FALSE
	T+5142	The server now evaluates all complex alarms containing /alarmpanel/VaultIntruderDetected and does not find any. It now considers processing complete.

(continued)

Table 8 Complex alarm walkthrough (Continued)

System clears pressure pad trigger	T+5508	The server changes the recorded state of /Vault1Cam/Triggers/Vault1Pad from TRUE to FALSE
	T+5532	The server now evaluates all complex alarms containing /Vault1Cam/Triggers/Vault1Pad and finds /PIRwithPADv1. This is a Boolean Logic AND expression between the recorded state of simple alarm /Vault1Cam/Triggers/Vault1PIR and the recorded state of alarm trigger/Vault1Cam/Triggers/Vault1Pad. This simplifies to FALSE AND FALSE which results in FALSE. The complex alarm /PIRwithPADv1 is marked as FALSE.
	T+5563	The server now evaluates all complex alarms containing /PIRwithPADv1 and finds /alarmpanel/VaultIntruderDetected. This is a Boolean Logic OR expression between the recorded states of /PIRwithPADv1, /PIRwithPADv2 and /PIRwithPADv3. Since all of these complex alarms have a recorded state of FALSE, then this simplifies to FALSE OR FALSE or FALSE which results in FALSE. The complex alarm /alarmpanel/VaultIntruderDetected is marked as FALSE
	T+5569	The server now evaluates all complex alarms containing /alarmpanel/VaultIntruderDetected and does not find any. It now considers processing complete.

Note: The technique of remembering the state of something, for example a simple alarm, for five seconds, is known as buffering. i.e. the TRUE state of a simple alarm is buffered as TRUE for five seconds following the firing of the simple alarm.

Chapter 7 – Accessing VSoIP Pro Remotely using a Web Browser

This chapter contains information on the following:

- Overview of Remote Access
- Prerequisites
- Using Remote Access

Overview of Remote Access

It is possible to remotely access a “light” version of VSoIP Pro from a web browser. Remote viewing allows you to:

- View live video
- View and navigate through recordings
- Select a screen layout

Caution: It is not necessary to have VSoIP Pro running to access the cameras remotely — the web client accesses the information stored on VSoIP Pro Server.

Prerequisites

To access VSoIP Pro remotely from a web browser, you must:

- Ensure the VSoIP Pro Server is running. To verify this, see the instructions in “Viewing Windows Services List” on page 148.
- Know the external IP address of the PC and the port number used by VSoIP Pro Server. To find out which port number is being used by VSoIP Pro Server’s Video Services service, from the Start menu, select VSoIPSuite Server>VSoIP Server Web-Client:
- A version of VSoIP Pro opens in a web browser. Note the port number shown in the address bar:

  A web page offering access to the server is displayed.

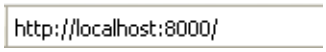


Figure 67 VSoIP Pro’s port number

Note: If the URL does not contain a port number, this indicates that the default port of 80 is being used by the VSoIP Pro Server.

- Configure the PC firewall to allow TCP/HTTP connections to be made to the Services.Service.exe application in C:\Program Files\GANZ\VSoIPSuite Server or switch it off.
- Have already added cameras. The remote interface does not provide a mechanism to add, edit or remove cameras.
- Have access to a second computer with Internet Explorer 8 and Microsoft Silverlight 3 or above installed. Follow this link on the second PC to install Silverlight 3 or above: http://www.microsoft.com/getsilverlight/get-started/install/default.aspx.

Using Remote Access

To access VSoIP Pro remotely using the second computer, enter the IP address and port number for the PC running VSoIP Pro.

For example: VSoIP Pro is running on a PC on a LAN with IP address 10.0.1.13. To view this from another PC on the same LAN, enter **`http://10.0.1.13:8000`** into the address bar of Internet Explorer on the second computer.

Note: The port number (the number after the colon) is only required if shown in the address bar — see above.

Note: If the port number indicated by the Event Properties dialog () is 80, you do not need to enter a port number in the address bar (the number after the colon in the address **`http://10.0.1.13:`*`8000`***).

Enter the user name and password you used to log into the VSoIP Pro Server and click Login.

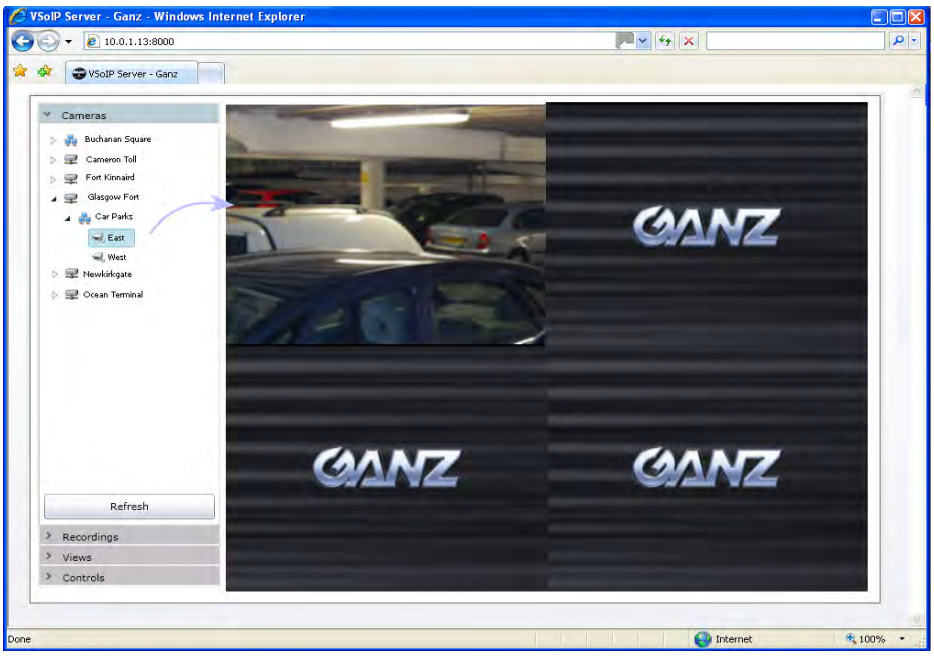


Figure 68 Viewing live video remotely

If this is the first time a remote access request has been made, then the first connection will take longer than subsequent requests. The remote access interface works in a similar way to that of the VSoIP Pro client.The pane on the left allows access to Cameras (live video).

- To view a live stream, click Cameras in the pane on the left. Click on the tree elements under Cameras until an encoder endpoint is shown. Drag this endpoint to an unoccupied view pane. The live video will take a short while to be shown. Once finished, click Controls and select Disconnect.
- To view a recording, click Recordings in the pane on the left. Click on the tree elements until an encoder endpoint is shown. Drag this from the Site Explorer to an unoccupied pane. The recorded video will take a short while to be shown. Once finished, click Controls and select Disconnect.

  Note: Only recordings which were specified as “Continuous” can be viewed remotely.
- To move around a recording, click Controls in the pane on the left.
  - Use the controls to move forwards and backwards in the recording, and to pause it.
  - To go to a particular time in a recording, click Go to Time and select the required options.

Figure 69 Controlling a recording in remote view

- To change the layout, click Views in the pane on the left and select the required display.

  Note: Any changes made using the remote viewer are not mirrored in the actual VSoIP Pro application.

Chapter 8 – Configuring PTZ Keyboards with VSoIP Pro

This chapter contains the following:

- Overview
- Installing the Hardware Keyboard Driver
- The Software Keyboard Driver
- Assigning Keyboard IDs

Overview

In addition to using a standard mouse to control video display, you can also use certain PTZ keyboards. For specific information on using particular keyboards, refer to the technical bulletin specific to that keyboard.

Before you can use a PTZ keyboard with VSoIP Pro, you must:

- Install the hardware keyboard driver. This is the driver that is shipped with the keyboard.
- Configure the software keyboard driver for use with VSoIP Pro. This is a driver which is shipped with VSoIP Pro, to allow it to work with the keyboard.
- Assign keyboard IDs to each remote client and device.

Prerequisites

The following software is required on the PC to which the keyboard is attached:

- Windows Installer 3.1
- Microsoft .Net Framework 3.5 SP1 (includes .Net frameworks 1.1, 2,0, 3.0 and 3.5). No configuration of the .Net Framework is required.

Note: These components are automatically downloaded from Microsoft during the installation process if not present at install time. They are also available from Microsoft's website as a download. Microsoft frequently redesigns its websites therefore an Internet download link is not provided. Instead we recommend that you use Google or another search engine to find the download links for the mandatory software. On examining the search results, please ensure that the download source is Microsoft.

- Microsoft Direct-X 9.0c or above. See "Direct-3D Hardware Support and Microsoft Direct-X 9.0c or above" on page 27 for more information on Direct-X.

Installing the Hardware Keyboard Driver

The keyboard driver is shipped with the keyboard. Installation varies from keyboard to keyboard. Please refer to the keyboard manufacturer's installation guide for driver installation instructions.

The Software Keyboard Driver

The keyboard software driver is installed during VSoIP Pro Installation. This installs a Windows Service called "PTZ Keyboard Service". This service must be running on the PC that has the keyboard connected to it. If no keyboard is required, this service can be safely stopped.

Starting and Stopping the Software Keyboard Driver

- To start the keyboard service, select Start>Programs>VSoIPSuite Client>Start PTZ Keyboard Service. This signals to the service that it should start up and run as a background task until the computer is shut down. When restarting the computer, the service will be signalled to start again and to remain running as a background task whenever the computer is running.
- To stop the keyboard service, select Start>Programs>VSoIPSuite Client>Stop PTZ Keyboard Service. This signals that the service should stop running as soon as possible. The service must be restarted after a reboot of the PC by selecting Start>Programs>VSoIP Suite Client>Start PTZ Keyboard Service.

Note: If you do not have a keyboard attached, please ensure that you do not inadvertently start the keyboard driver service as this may create irrelevant audit trail entries.

Configuring the Software Keyboard Driver

Before you can use the keyboard with VSoIP Pro, you must configure the software keyboard driver so that the keyboard is recognised by VSoIP Pro. To do this:

1 Navigate to the VSoIP Pro Client installation directory (normally C:\Program Files\GANZ\VSoIPSuite Client).

2 Locate and double-click the Keyboard.Config.exe file.

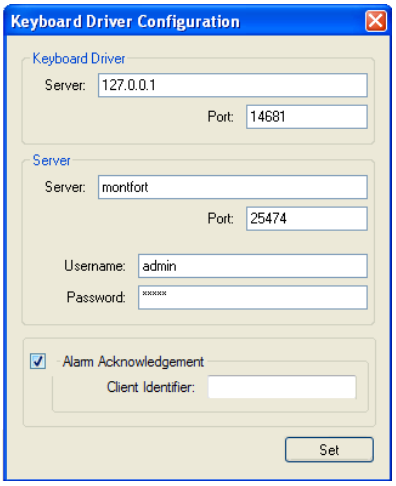


Figure 70 Configuring the keyboard driver

3 Under Keyboard Driver, enter the IP address of the PC to which the keyboard is attached. By default, this is set to 127.0.0.1. If a specific port number other than the default (14681) must be used, enter this here.

4 Under Server, enter the IP address (or name) of the server with which the keyboard will be used. If a specific port number other than the default (25374) must be used, enter this here.

5 Enter the user name and password used to log in to the selected server.

Note: If these user login details are changed from within VSoIP Pro, the keyboard will be unable to connect. To update the login details used by the keyboard, open the Keyboard Driver Configuration tool again change the login details as required.

To avoid this issue, we recommend that you create an explicit keyboard user with appropriate permissions, which can be reserved explicitly for use by the keyboard. Please see “Setting Passwords for Video-wall and PTZ Keyboard Users” on page 32 for more information.

6 You can then specify which client alarm acknowledgements are sent to. By default the alarm acknowledge button on the keyboard sends alarm acknowledgments to the currently selected client. If you want these acknowledgements to be sent to a specific client, check the Alarm Acknowledgement box and enter the ID of the client to which acknowledgements are to be sent. This means that if an alarm appears in the alarm stack of a particular client, pressing the Acknowledge keyboard button acknowledges that alarm.

7 Click Set.

8 Start the PTZ Keyboard Service. For details on how to do this, see “Viewing Windows Services List” on page 148.

Note: Once the PC has been restarted, this service should start automatically with the VSoIP Pro client.

Caution: If you uninstall and reinstall the VSoIP Pro client, you must re-enter the keyboard access details by re-configuring the keyboard software driver.

Assigning Keyboard IDs

To use a PTZ keyboard, keyboard identifiers must be assigned to all devices, remote clients, Video-walls, and Display clients that will be used by the keyboard.

Note: The device to which the keyboard is attached must also be added.

You can either have VSoIP Pro allocate IDs automatically, or allocate them manually.

Automatic Allocation

To have keyboard IDs assigned automatically by VSoIP Pro, click Auto Assign IDs.

Caution: Clicking Auto Assign IDs assigns IDs to all devices and remote clients in the site for use with PTZ keyboards. Once IDs have been assigned, they can only be removed by deleting the ID for each device individually.

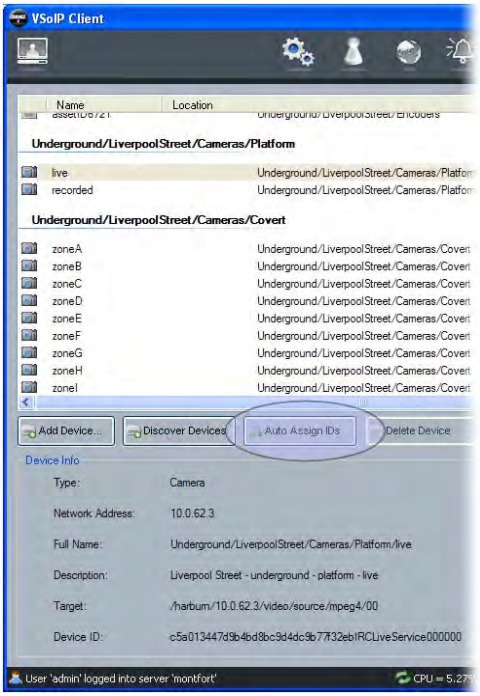


Figure 71 Automatically assigning keyboard IDs

Each client and device in the site is allocated a unique ID for use with the keyboard.

Manual Allocation

To manually allocate keyboard IDs to individual devices (including Video-walls) or remote clients, double-click the required item in the list, and enter a number in the Keyboard Identifier field, as shown below. Click Update to apply the change.

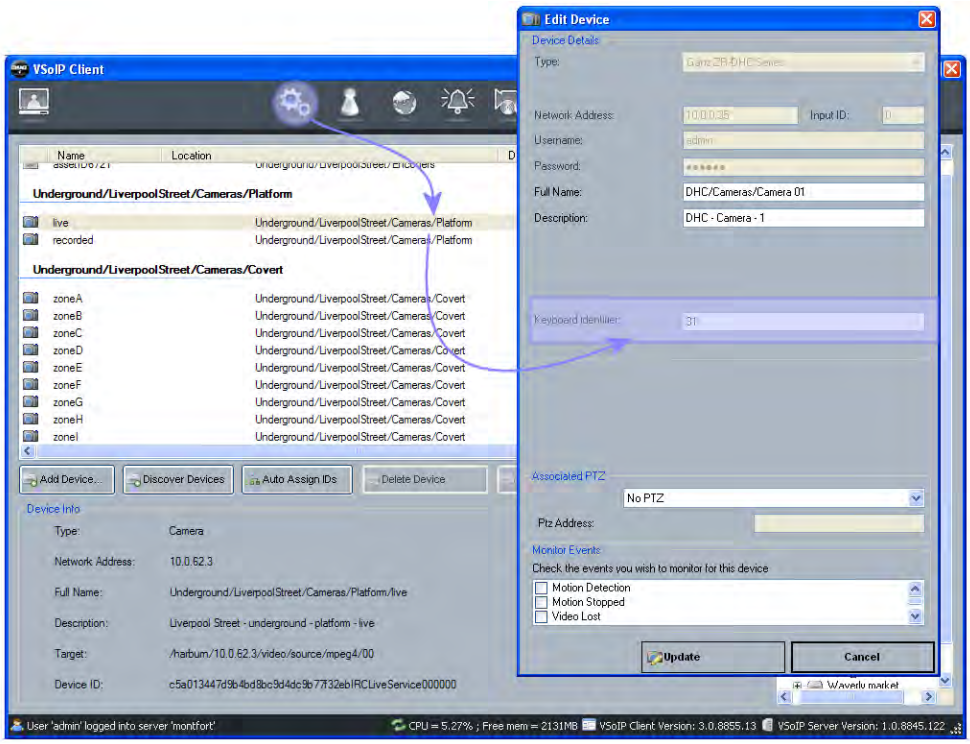


Figure 72 Manually assigning keyboard IDs to a camera

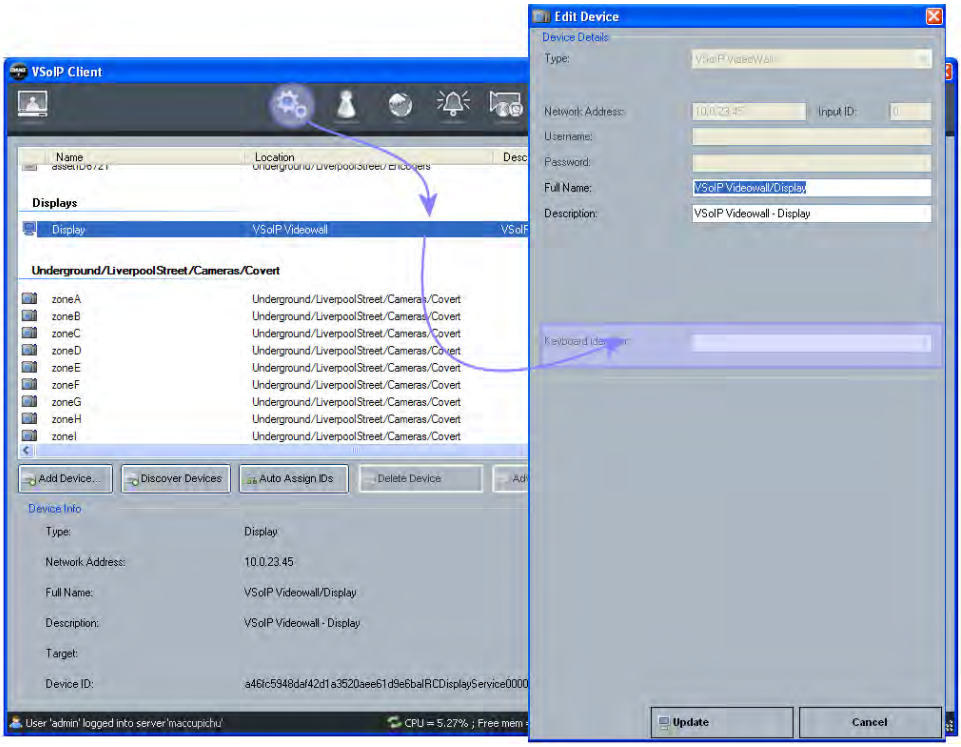


Figure 73 Manually assigning keyboard IDs to a Video-wall

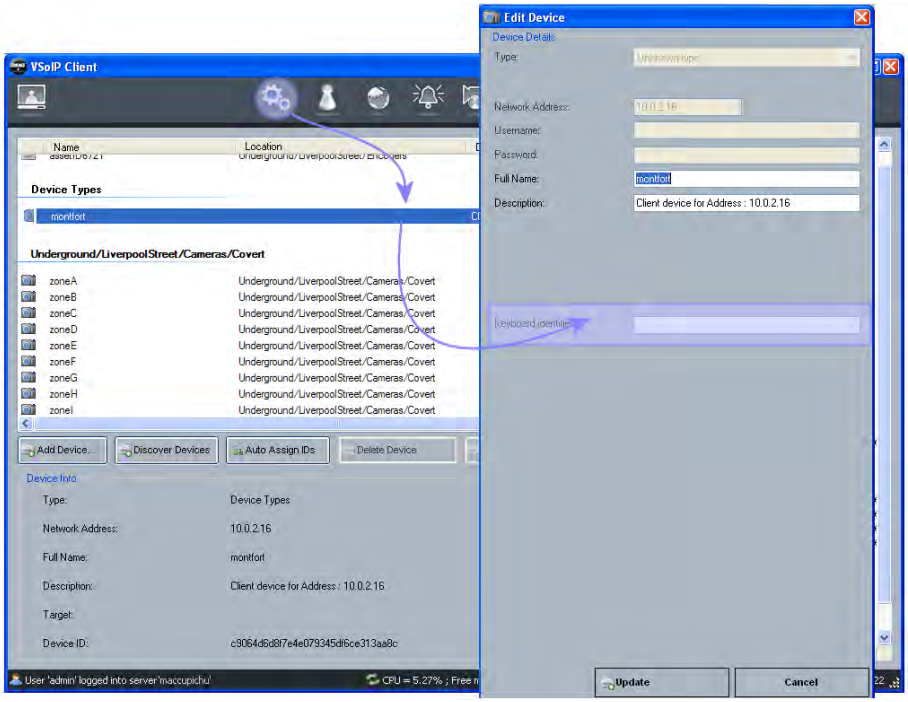


Figure 74 Manually assigning keyboard IDs to a remote client

Using the Keyboard to View Video

For information on how to use the keyboard to view video, please see Chapter 9, "Using PTZ Keyboards with VSoIP Pro".

Chapter 9 – Using PTZ Keyboards with VSoIP Pro

This chapter contains the following information:

- Identifying Devices and Video Panes
- Using a PTZ Keyboard
- Troubleshooting PTZ Keyboards

Getting Started

To use a PTZ keyboard, the PTZ Keyboard Service must be running. To start the service, from the Start menu, select VSoIP Pro>Start PTZ Keyboard Service.

Identifying Devices and Video Panes

To identify which number has been allocated to each video pane and device, press the Identify Pane button on your keyboard. This displays an overlay on all visible panes and devices in the tree indicating what their assigned IDs are, that is, their "pane number" or "camera number". These are used when using the keyboard as described below.

Note: Please refer to the technical bulletin specific to your keyboard for the location of the Identify Pane button.

Using a PTZ Keyboard

The following table details which button presses are required to carry out certain tasks using a keyboard. Please refer to the technical bulletin specific to your keyboard for how these presses map to the physical buttons on your keyboard.

To do this...	...press these keys
Select a pane	[SELECT PANE]<pane number>[ENTER]
View a camera in a pane	[SELECT CAMERA]<camera number>[ENTER]
Switch to playback mode	[START PLAYBACK] *
Acknowledge the first alarm in the alarm stack	[ACKNOWLEDGE ALARM]
Enable PTZ in pane	[TURN ON PTZ]
Control PTZ	[TURN ON PTZ], then use joystick
Enable digital zoom	Use joystick
Identify devices and monitors	[IDENTIFY PANE]
Go to PTZ preset (when PTZ is enabled)	[SELECT PTZ PRESET]<preset number>[ENTER]
Start PTZ tour (when PTZ is enabled)	[SELECT PTZ TOUR]<tour number>[ENTER]
Cancel input (e.g. monitor, keyboard)	[CANCEL]
Disconnect	[DISCONNECT CAMERA]

To clear any messages from the screen, press [ENTER].

* Playback starts five minutes before the end of the most recent recording.

Troubleshooting PTZ Keyboards

- If VSoIP Pro cannot access a PTZ keyboard, please check that the PTZ Keyboard Service is running. For details on how to do this, see “Viewing Windows Services List” on page 148. If the service is not running, from the Start menu, select VSoIP Pro>Start PTZ Keyboard Service.
- If you cannot view a particular camera on screen using the keyboard, please check that the user logged in to the client has permission to view this camera. For example, if a user logged into Client B does NOT have permission to display camera A, then video from camera A will not be displayed on Client B.

Chapter 10 – Designing Mapsets

This chapter contains information on the following:

- Mapsets Overview
- Designing Mapsets
- Creating a Mapset without a Map Design Tool

Mapsets Overview

Caution: To use mapsets, you must open port 8080 for both server and client components. For more information, see the chapters on server and client installation.

If you are using Microsoft Internet Explorer version 8, you must add the IP address or network name of the server computer to the list of trusted computers in Internet Explorer. For more information, see “Adding Trusted Sites” on page 26.

A mapset is similar to a mini-website; it is a collection of interconnected pages or “maps” that contain links to various surveillance system components. Similar to the Web, mapsets can contain a mix of text and graphic parts.

Mapsets are often used as an alternative view to the hierarchical, branched tree representation of system components observed in the client.

Mapsets are an opportunity to present the site in a manner familiar to the operators of the system. For example a member of a CCTV operator’s group might have access to a mapset or a series of mapsets showing the physical layout of the site they are monitoring, i.e. it contains a graphical site-map, a site plan showing various named buildings and floor plans of the various buildings. These various parts are most likely to be shown over several interconnected pages. Links between pages could be specially marked areas over the buildings, the floor plan etc. Alternatively a mapset for an installer might be a series of system wiring diagrams allowing the engineer to troubleshoot device issues without the need to understand the physical location of a devices.

The similarity between mapsets and websites can also be seen by viewing the pages making up a mapset in a text editor, are seen as a series of pages containing textual content formatted and following the rules of XHTML as managed and publicised by the World Wide Web Consortium.

For more details and on-line tutorials about creating XHTML documents valid as mapsets please visit the World Wide Web Consortium’s website and compare the details there with the sample mapsets installed alongside the client in the client’s installation folder.

World Wide Web Consortium XHTML (http://www.w3.org/TR/xhtml1/)

Designing Mapsets

You should consider the following when planning a mapset:

- Is the mapset for CCTV operators, or for maintenance personnel? This drives the style of the content.
- Is a single page enough, or will multiple pages be required?
- Is the size of each page background image suitable for the PC display resolution in use by the clients? Large images could be broken into smaller images and become backgrounds on interconnected pages.
- Do you have a list of the devices that should be present on the map?
- Are the images in a format suitable for inclusion on a page? Images should be in .GIF, .JPG or .PNG format.

Ideally, a mapset design tool should be used to create the mapset, such as Amaya 11.3 XHTML Map Editor, available from vsoip.cbceurope.eu. However, you can also create mapsets manually using Windows Notepad, as explained below.

Creating a Mapset without a Map Design Tool

A mapset is a set of one or more map pages that provide the user with an alternative method of using the surveillance system.

If the system installer, administrative level user, or user with mapset addition privileges plans to create a mapset and they do not have access to a map design tool for the surveillance system, they can create mapsets using:

- Windows Notepad — The Windows notepad application has sufficient capabilities to create and maintain map pages. This is accessed from the Start menu>All Programs>Accessories>Notepad.
- File Compression Utility — This is used to collect map pages and, optionally, graphical content, into a single archive file. This is also known as a compressed folder. A compressing application is built in to the operating system but if preferred third-party, standalone applications such as WinZIP or WinRAR can be used.
- Graphical editor (optional) — This is useful for creating the page background. Editors that show the position of the mouse relative to the upper-left corner of a loaded image are useful when calculating positions for map graphics such as camera or alarm icons.
- Internet Explorer (optional) — This is useful for accessing services such as those for Globally Unique Identifier (GUID) generation, for example http://guidgen.com.
- GUID generator application (optional) — Several third party GUID generator applications can be downloaded from the Internet. Since links always change none is included here - perform an Internet search to find a suitable application.

It is within the means of most engineer grade personnel to use these instructions along with some study of basic web-page construction to create powerful and useful mapsets. This section cannot however teach all that is required to create XHTML pages. This section is written as a guide to those already familiar with HTML and web page construction. It is recommended that some study of web-page design using HTML is carried out for those who are not familiar.

Typical Workflow

The server requires that the individual pages that constitute a single mapset are collected together in a single file. This file is an archive generated by any archive generating tool that can produce ZIP format files.

The structure of the archived file system, e.g. the files and folders that are contained in the ZIP archive, is flexible, however each archive MUST contain a single file called index.html at the top-level of the archived folder hierarchy, as shown below.

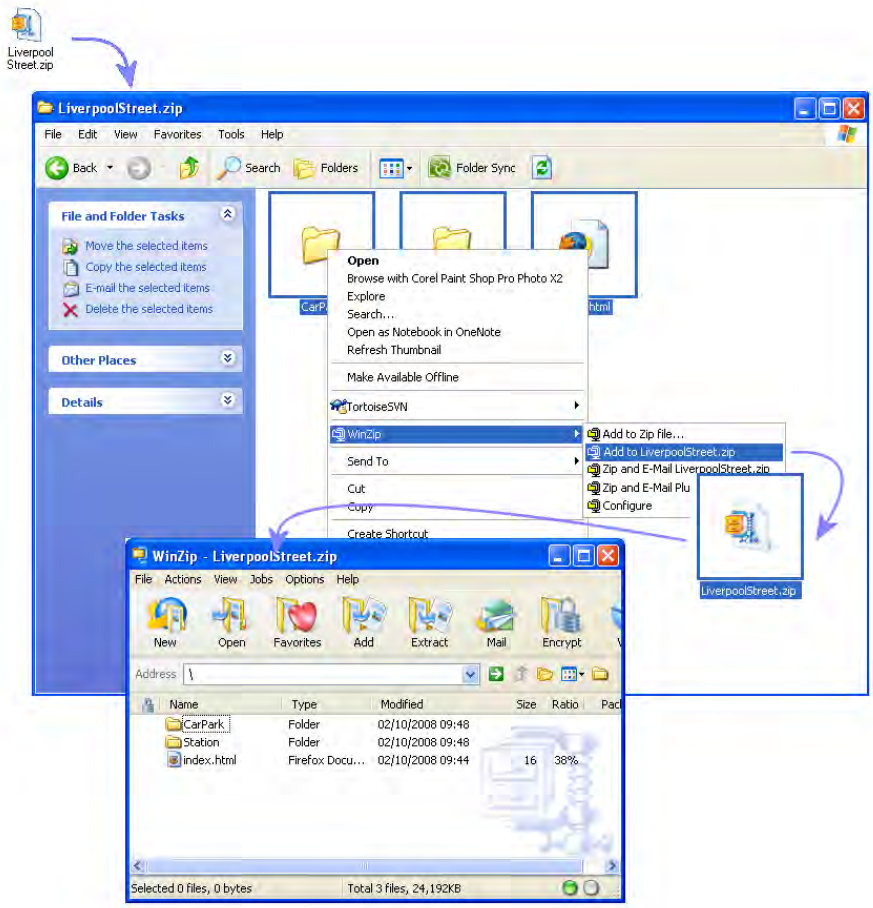


Figure 75 Internal structure of mapset zip file

The mapset creator decides on the layout of the mapset, or mapsets that will be used. A mapset itself is a collection of one, or more map pages. The user navigates a mapset entering at the home page, which has file name index.htm, and jumps to other map pages using anchor links added to a map page.

When designing mapsets, you should consider the following:

- Always have a page link from any page back to the home page of the mapset.
- Adding *previous* and *next* map history links can allow for quick navigation.
- You can aid navigation by adding page links to other map pages to the home page.

  For example, if you have a mapset with a home page and pages called:

  - floor 1
  - floor 2
  - roof
  - basement

  You may find navigation easier if you add links to floor 1, floor 2, roof, basement to the home page rather than adding links to floor 1 and basement to the home page, but links to floor 2 on the floor 1 map page, and to roof on floor 2 map page.
- Use map-page background images to add detailed content, but always size these to match the screen area (in pixels) of the map window shown by the PCs running the surveillance client used to view map pages. For example, the client PC has a 1280 x 1024 pixel monitor, but the area most likely to be used for map display on that monitor will typically be 640x480 pixels, with other video, and client application user interface taking up the remaining area. Thus, making background images 640 x 480 will mean that users will not need to scroll to see the map content.

- Split content rich, dimensionally large backgrounds images down into several dimensionally smaller background images. Use these dimensionally smaller images as the background on several interconnected map pages with page links connecting adjacent pieces of the divided background. This is better than scaling a dimensionally large image smaller with the resultant lack of detail and clarity.
- Ensure that images are 72dpi and not higher, since higher dpi will not necessarily improve map background clarity, but will unnecessarily add to the system memory consumed on surveillance clients and possibly slow down client log-in and mapset page loading performance.

The following workflow is suggested:

1 Make a list of all the map pages that will be needed.

2 Obtain background images for each, scaling or sub-dividing as necessary.

3 Consider which map page will be the home page.

4 Obtain suitable images for camera icons and alarm icons as required.

5 Calculate the coordinates relative to top-left of background image where camera and alarm icons should be placed.

6 Using the notepad application, create a placeholder page for each map required using the standard map page content shown below, saving the map chosen as the home map as index.htm and the others with memorable names related to the custom map page content to be added. All text files saved by the Notepad application should be in the same folder and all have the file extension .htm.

Placeholder Map Page

The placeholder map page is a text file, saved with .htm extension, containing the bare minimum content to be a valid map page. The page will not display any content if added to a mapset but contains all mandatory elements required to be uploaded to the surveillance suite server and to be displayed by surveillance suite clients.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>PLACEHOLDER PAGE CHANGE ME</title>
      <meta http-equiv="content-type" content="text/html; charset=utf-8" />
  </head>
  <body style="background-color:#ffffff">
    <div style="position:absolute;height:97%;width:97%">
      <div
        style="margin-left:-320px; margin-top:-240px;position:relative;
               left:50%;top:50%;">
        <img alt="PLACEHOLDER BACKGROUND" title=" PLACEHOLDER BACKGROUND"
          src="VgaBackgroundImage.png"
          style="left: 0px; position: absolute; top: 0px;
          width:640px; height: 480px;" />
      </div>
    </div>
  </body>
</html>
```

The page placeholder assumes that a background image called VgaBackgroundImage.png has been created and placed in the same folder as this file. Notice that there are width and height style attributes that match the size of the VgaBackground.png image i.e. 640 pixels wide by 480 pixels high.

Importantly notice also immediately prior to the <img /> XHTML tag that describes the VgaBackground.png image, there is a tag which has a style attribute detailing a left and top margin. This is half the size of the height and width of the background image.

When changing the background image to another image make sure that you change the value representing the background images filename src="VgaBackgroundImage.png" to the appropriate name of the background image. Also change the value of the height and width style attributes to match that of the new image. Finally change the left and top margin style attribute values to a half of the height and width of the image.

Caution: The margin-left and margin-top tag's style attribute values should be negative values. Only change the number part of these values and leave the sign unchanged.

Page Links - Textual

A page link causes the map page to switch to the new page described by the link. The XHTML content to do this is known as the anchor, or <a>, tag.

To link from a map page to the home page, the following XHTML statement can be placed within the <body></body> content of that map page.

```
<a href="index.htm">Home page</a>
```

Note: The anchor (or page link) tag cannot appear between <object> and </object> tags.

To link from a page to another page, the following XHTML statement can be placed using the same rules listed above.

```
<a href="floor1.htm">Go to floor ONE</a>
```

Camera Links - Graphical

A camera link is a graphical object on a map that is used to show an alternative view of the IP cameras and encoders described in the surveillance site. A user can interact with the camera link to perform operations on the IP camera or encoder associated with the link, typically this would be to view video from the camera.

A camera link has the following attributes:

- Name (required) — A short but descriptive name for the camera. The name should not start with a number, should contain only letters or numbers and cannot include spaces.
- Description (optional) — A longer descriptive name for the camera. The name should contain only letters, numbers and spaces.
- Camera image (required) — A 256 colours, or greater, JPEG or PNG format graphic of 48x48 pixels in width and height.
- Map position (required) — The coordinates on the map background where the upper-left hand corner of the camera link image should appear.

  The x-coordinate starts at 0 at the extreme left of the background and counts up one unit at time until the maximum value, near the extreme right of the background image. This maximum is the width of the background graphic in pixels minus the width of the camera image.

  The y-coordinate starts at 0 at the extreme top of the background and counts up one unit at time until the maximum value which is near the extreme bottom of the background image. This maximum is the height of the background graphic in pixels minus the height of the camera image.
- Unique element ID (required) — A precisely formatted identifier called a Globally Unique Identifier, or GUID.

The user of the map sees only the following attributes:

- Camera image.
- Position — the image appears on map at the position specified.
- Dimensions — the image is scaled to the size given.

Note: For a user to interact with the camera images, the user must have permissions to view the camera associated with the camera link. If the user does not have permission, they will always see the camera image irrespective of whether they are permitted to interact with that camera.

The administrator of the system sees only the camera link name attribute during mapset configuration. The administrator uses the names of IP cameras and encoders and the names of the camera links to associate the cameras with the camera links.

Defining a Graphical Camera Link

Note: If you are using Microsoft Internet Explorer 8 or later to view maps, you must add the server computer IP address or network name to the list of trusted computers to ensure that camera and alarm links appear on maps. For information on how to do this, please see “Adding Trusted Sites” on page 26.

Camera links make use of an XHTML expression all contained within an Object tag.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Camera link example</title>
      <meta http-equiv="content-type" content="text/html; charset=utf-8" />
  </head>
  <body style="background-color:#ffffff">
    <div style="position:absolute;height:97%;width:97%">
      <div
        style="margin-left:-320px; margin-top:-240px;position:relative;
               left:50%;top:50%;">
        <img alt="Camera link example" title="Camera link example"
          src="VgaBackgroundImage.png"
          style="left: 0px; position: absolute; top: 0px;
          width:640px; height: 480px;" />
        <object title="Upper left corner VGA sized map"
          style="left: 0px; position: absolute; top: 0px;"
          id="4300bcd547364605977dad65db231504"
          classid="RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapCamera"
          width="48" height="48">
         <param name="ObjectID" value="CameraUpperLeft" />
         <param name="ImageUrl" value="TopLeft.png" />
         <img
           src=""
           title="Upper left corner VGA sized map"
           alt="Upper left corner VGA sized map" />
        </object>
        <object title="Upper right corner VGA sized map"
          style="left: 599px; position: absolute; top: 0px;"
          id="bfe3c1fcab164b2ca8e38a8165e7c6d0"
          classid="RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapCamera"
          width="48" height="48">
         <param name="ObjectID" value="CameraUpperRight" />
         <param name="ImageUrl" value="TopRight.png" />
         <img
           src=""
           title="Upper right corner VGA sized map"
           alt="Upper right corner VGA sized map" />
        </object>
        <object title="Lower left corner VGA sized map"
          style="left: 0px; position: absolute; top: 439px;"
          id="6d6156b22f2d4ba6b7653e1f6a8597f2"
          classid="RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapCamera"
          width="48" height="48">
         <param name="ObjectID" value="CameraLowerLeft" />
         <param name="ImageUrl" value="LowerLeft.png" />
         <img
           src=""
           title="Lower left corner VGA sized map"
           alt="Lower left corner VGA sized map" />
        </object>
        <object title="Lower right corner VGA sized map"
          style="left: 599px; position: absolute; top: 439px;"
          id="62781b4a4f8c40438c933b5db3566391"
          classid="RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapCamera"
          width="48" height="48">
         <param name="ObjectID" value="CameraLowerRight" />
         <param name="ImageUrl" value="LowerRight.png" />
         <img
           src=""
           title="Lower right corner VGA sized map"
           alt="Lower right corner VGA sized map" />
        </object>
      </div>
    </div>
  </body>
</html>
```

The content shown above is an example of a complete map page. It was created in Windows Notepad. In this example the map page is the file index.htm, The name is relevant here as index.htm is the "entry point" or home page of a mapset.

Ordinarily this file, along with other map pages and images would be held in a single zip archive file, renamed to have a .mapset filename so that it could be loaded into the surveillance suite.

Study the content shown above. The content shown outside the sections bounded by the <object> and </object> XHTML tags is common to all map pages. Typically the text between the <title> and </title> XHTML tags is changed to suit the purpose of each map page, e.g. Ground Floor, Car-park, Lobby etc.

On map pages, a pair of object tags, <object></object> surrounds each camera link. Each object has the following attributes:

- Title — A longer descriptive name for the camera. The name should contain only letters, numbers and spaces.
- Position — An offset from the left and an offset from the top of the map page in pixels.
- Width — The maximum width in pixels of the camera image.
- Height — The maximum height in pixels of the camera image.
- Id — A system wide unique GUID for this camera link as generated from a GUID generator service like http://guidgen.com or from a GUID generating application.

  Note: The GUID must only contain letters and numbers. Any hyphen characters should be removed.
- classid — Must be set to `RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapCamera`.
- ObjectID — The name of the camera link: a short but descriptive name for the camera. The name should not start with a number, should contain only letters or numbers and cannot include spaces.
- ImageUrl — The filename of a .PNG or .JPG graphic representing the camera. The filename must include a file path relative to the folder containing the map file.

  Notice that the textual content associated with the title attribute is repeated in the <img /> tag as values for the img tag's "title" and "alt" attributes.

Note: This section contains details of adding camera links to a map page. There is additional page content that is not shown in this subsection that describes page artwork and region, text and alarm links. Also, the process of adding the created page to a zip archive so it becomes a part of a mapset is not described here.

Caution: The `RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapCamera` classid must be used whenever an object is to be associated with a camera link.

Alarm Links

An alarm link is a graphical object on a map that can be used to show the state of an alarm within the surveillance system.

An alarm link has the following attributes:

- Name (required) — a short but descriptive name for the alarm. The name should not start with a number, should contain only letters or numbers and cannot include spaces.
- Description (optional) — a longer descriptive name for the alarm. The name should contain only letters, numbers and spaces.
- Inactive image (required) — A 256 colours, or greater, JPEG or PNG format graphic of 48x48 pixels in width and height.
- Active image (required) — A 256 colours, or greater, JPEG or PNG format graphic of 48x48 pixels in width and height.
- Flash image (required) — A 256 colours, or greater, JPEG or PNG format graphic of 48x48 pixels in width and height.
- Map position (required) — The coordinates on the map background where the upper-left hand corner of the alarm link image should appear.

The x-coordinate starts at 0 at the extreme left of the background and counts up one unit at time until the maximum value which is near the extreme right of the background image. This maximum is the width of the background graphic in pixels minus the width of the alarm image.

The y-coordinate starts at 0 at the extreme top of the background and counts up one unit at time until the maximum value which is near the extreme bottom of the background image. This maximum is the height of the background graphic in pixels minus the height of the alarm image.

- Unique element ID (required) — A precisely formatted identifier called a Globally Unique Identifier, or GUID.

The user of the map sees only the following attributes:

- Inactive image — when the alarm source associated with the alarm is in the acknowledged or closed state.
- Active image — when the alarm source associated with the alarm is in the unacknowledged state - and the flash image is not currently displayed.
- Flash image — when the alarm source associated with the alarm is in the unacknowledged state - and the active image is not currently displayed.
- Position — one of the images appears on map at the position specified.
- Dimension — the images are scaled to the size given

Note: For a user to see the active and flash alarm images representing an alarm link, they must have permissions to view alarms for the alarm source associated with the alarm link. If the user does not have permission, they will always see the inactive image irrespective of the state of the alarm within the system.

The administrator of the system sees only the alarm link name attribute during mapset configuration. The administrator uses the names of alarm sources and the names of the alarm link to associate the alarm source to the alarm link.

Defining an Alarm Link

Note: If you are using Microsoft Internet Explorer 8 or later to view maps, you must add the server computer IP address or network name to the list of trusted computers to ensure that camera and alarm links appear on maps. For information on how to do this, please see “Adding Trusted Sites” on page 26.

Adding an alarm link to a map page is similar to the process of defining a camera link. Alarm links make use of an XHTML expression all contained within an Object tag.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Alarm link example</title>
      <meta http-equiv="content-type" content="text/html; charset=utf-8" />
  </head>
  <body style="background-color:#ffffff">
    <div style="position:absolute;height:97%;width:97%">
      <div
          style="margin-left:-320px; margin-top:-240px; position:relative;
                 left:50%;top:50%;">
        <object title="Alarm link example"
          style="left: 320px; position: absolute; top: 240px;"
          id="2abd95e739874c338a4adaa3a504be3b"
          classid="RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapAlarm"
          width="48" height="48">
         <param name="ObjectID" value="AlarmNameGoesHere" />
         <param name="ActiveImageUrl" value="alarm_active.PNG" />
         <param name="InactiveImageUrl" value="alarm_inactive.PNG" />
         <param name="ActiveFlashImageUrl" value="alarm_active_flash.PNG" />
         <img src="" title="Alarm link example" alt=" Alarm link example" />
        </object>
      </div>
    </div>
  </body>
</html>
```

The content shown above is an example of a complete map page. It was created in Windows Notepad. In this example the map page is the file index.htm. The name is relevant here as index.htm is the "entry point" or home page of a Mapset.

Ordinarily this file, along with other map pages and images would be held in a single zip archive file, renamed to have a .mapset filename so that it could be loaded into the surveillance suite.

Study the content shown above. The content shown outside of the section bounded by the <object> and </object> XHTML tags is common to all map pages. Typically the text between the <title> and </title> XHTML tags is changed to suit the purpose of each map page, e.g. Ground Floor, Car-park, Lobby etc.

On map pages, a pair of object tags, <object></object> surrounds each alarm link. Each object has the following attributes:

- Title — A longer descriptive name for the alarm. The name should contain only letters, numbers and spaces.
- Position — An offset from the left and an offset from the top of the map page in pixels.
- Width — The maximum width in pixels of the active, active flash and inactive images.
- Height — The maximum height in pixels of the active, active flash and inactive images.
- Id — A system wide unique GUID for this alarm link as generated from a GUID generator service like http://guidgen.com or from a GUID generating application.

  Note: The GUID must only contain letters and numbers. Any hyphen characters should be removed.
- classid — must be set to `RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapAlarm`
- ObjectID — The Name of the alarm link: a short but descriptive name for the alarm. The name should not start with a number, should contain only letters or numbers and cannot include spaces.
- ActiveImageUrl — The filename of a .PNG or .JPG graphic representing an unacknowledged alarm when it is being shown in the not flashing state. The filename must include a file path relative to the folder containing the map file.
- ActiveFlashImageUrl — The filename of a .PNG or .JPG graphic representing an unacknowledged alarm when it is being shown in the flashing state. The filename must include a file path relative to the folder containing the map file.
- InactiveImageUrl — The filename of a .PNG or .JPG graphic representing an unacknowledged alarm when it is being shown in the not flashing state. The filename must include a file path relative to the folder containing the map file.

Notice that the textual content associated with the title attribute is repeated in the <img /> tag as values for the img tag's "title" and "alt" attributes.

Note: This section contains details of adding alarm links to a map page. There is additional page content that not shown in this subsection that describes page artwork and region, text and camera links. Also, the process of adding the created page to a zip archive so it becomes a part of a mapset is not described here.

Caution: The `RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapAlarm` classid must be used when an object is to be associated with an alarm link.

Chapter 11 – Configuring and Using Mapsets

This chapter contains information on the following:

- Adding Mapsets to the Server
- Associating Map-links with Devices
- Deleting Mapsets
- Troubleshooting
- Using Mapsets

Introduction

Mapsets are a collection of hypertext marked-up documents archived in a zip file format archive. See “Designing Mapsets” on page 99 for more details about mapsets and their construction.

Note: The following sections assume that a valid mapset has been created.

Adding Mapsets to the Server

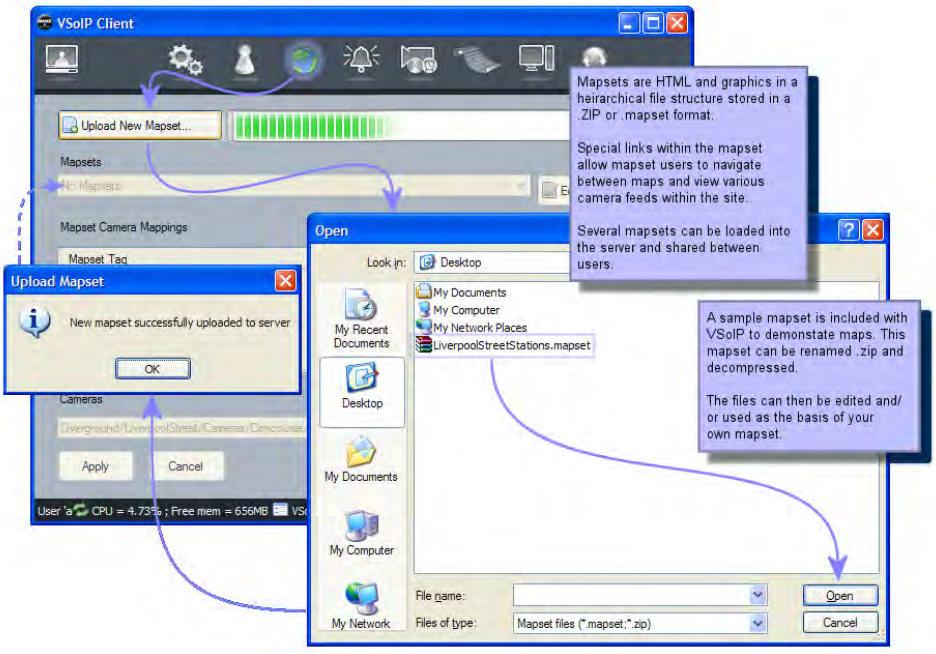

VSoIP Client
Upload New Mapset...
Mapsets
Mapset Camera Mappings
Mapset Tag
Upload Mapset
New mapset successfully uploaded to server
OK
Cameras
Apply
Cancel
Mapsets are HTML and graphics in a heirarchical file structure stored in a .ZIP or .mapset format.
Special links within the mapset allow mapset users to navigate between maps and view various camera feeds within the site.
Several mapsets can be loaded into the server and shared between users.
Open
Look in:
Desktop
My Documents
My Computer
My Network Places
LiverpoolStreetStations.mapset
My Recent Documents
Desktop
My Documents
My Computer
My Network
File name:
Files of type:
Mapset files (*.mapset;*.zip)
Open
Cancel
A sample mapset is included with VSoIP to demonstate maps. This mapset can be renamed .zip and decompressed.
The files can then be edited and/or used as the basis of your own mapset.

Figure 76 Uploading mapset on disk to server

Note: If you have made changes to an existing mapset, and then upload the new version, you are prompted to confirm that you want to overwrite the old mapset. Note that links in the old mapset are maintained as far as possible.

Associating Map-links with Devices

When creating a mapset, you may have added map-links, such as camera icons, at certain places on mapset pages. You can now associate these links with devices. For example, you may want live video to be displayed when you click a camera icon.

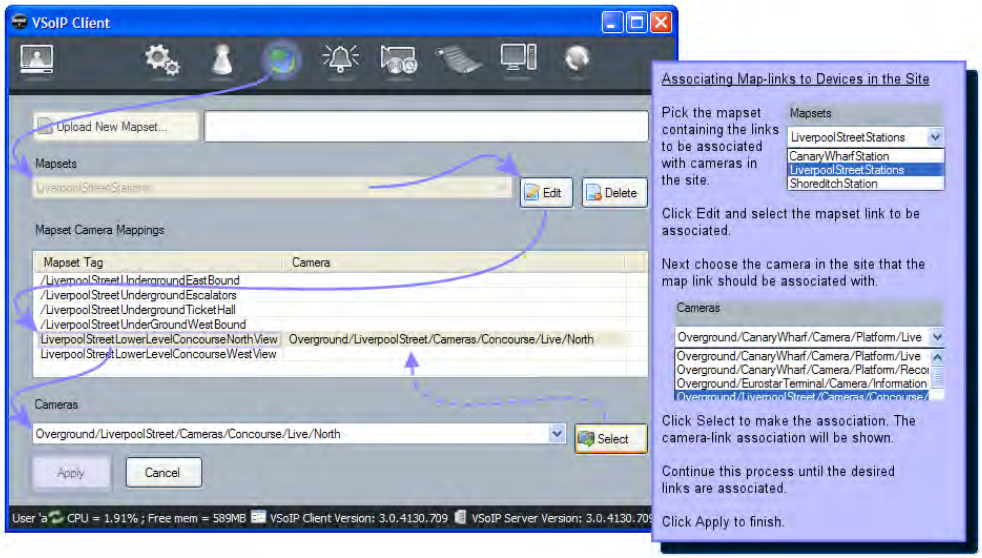


Figure 77 Assigning map-links to devices within site

Deleting Mapsets

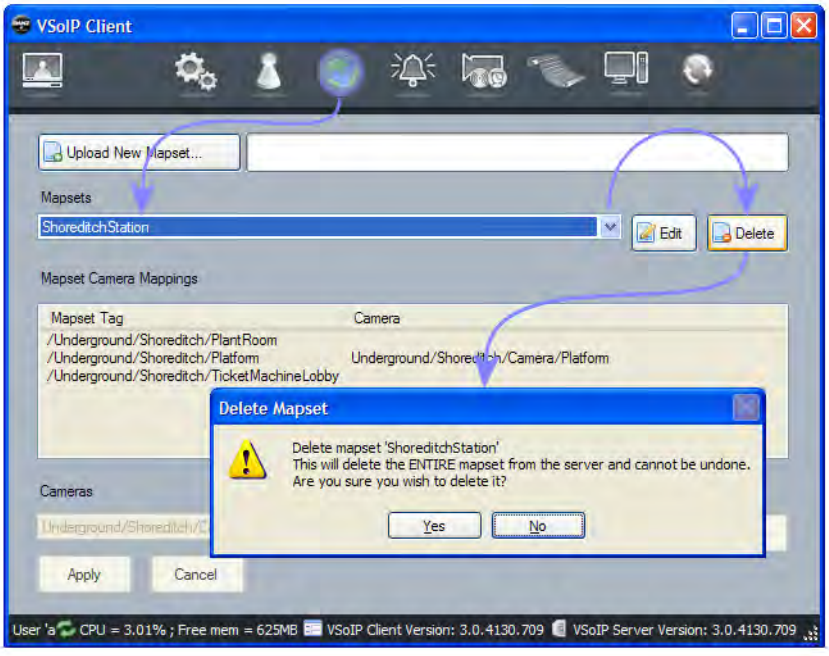


Figure 78 Deleting mapsets from server

Troubleshooting

My Configuration Changes have not been Saved

On rare occasions, it is possible that you may experience problems when saving configuration changes. It may be that VSoIP Pro will fail to save such changes to its configuration files. This could happen if the configuration files are held on another machine and a networking problem occurs.

When saving configuration changes, VSoIP Pro carries out the following steps:

1 Copies the working file to a backup (named <file>-old).

2 Writes the changes to a temporary file (named <file>-temp)

3 Copies the temporary file to the working file.

4 Deletes the temporary and backup files.

The <file> notation refers to one of several configuration files that are held in the VSoIP "conf" directory, which is created during installation.

If a problem occurs, some of these steps may not take place. VSoIP Pro attempts to copy the backup file back to the working file but even this may fail if there are file access problems. The best way to resolve the issue is to restore file access and attempt the configuration save again. This brings the working file into sync and deletes the temporary and backup files.

Using Mapsets

Once you have designed and uploaded your mapset(s) to the server, you can start using them. This section considers a sample mapset, entitled LiverpoolStreetStations, which consists of three map pages.

Figure 79 shows the home page of the mapset. Here, links have been created for East Bound, West Bound, Ticket Hall and Escalators. There are two ways to access the lower level for the overground station — either clicking on Liverpool Street on the map, or using the “lower level” link.

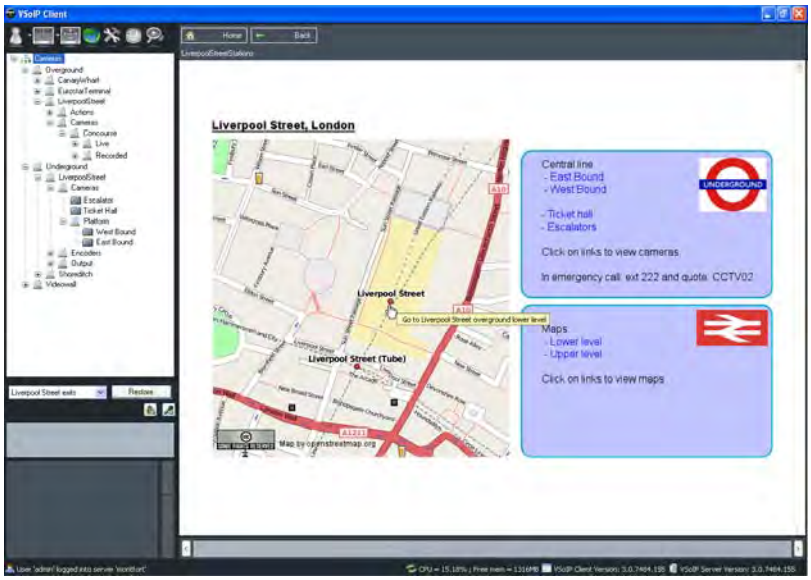


Figure 79 Home page for Liverpool Street mapset

Clicking this lower level link opens up another map (Figure 80):

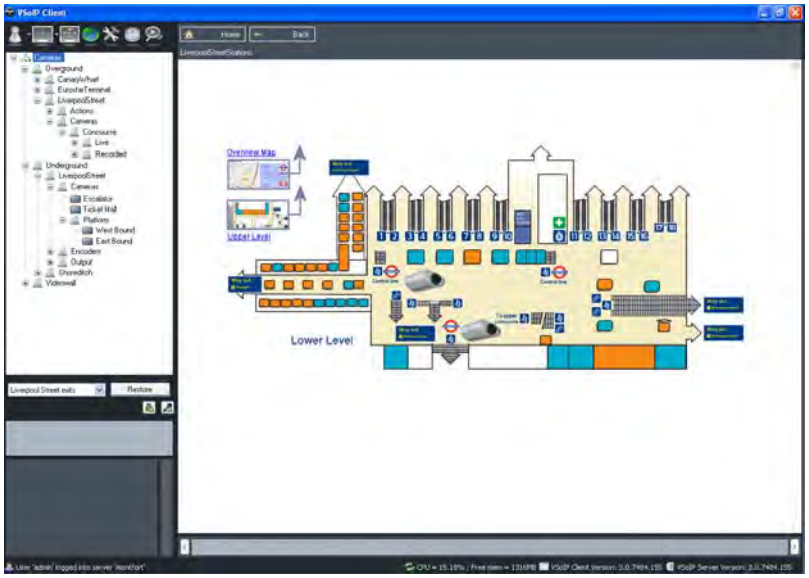


Figure 80 Liverpool Street mapset — lower level

Here, links have been provided to the overview and upper level maps to improve accessibility. The camera icons represent cameras on site. Click an icon to view live video from that device in a separate popup window.

- If you are using a dual-head monitor you can display video from camera links in the second monitor. Select a video pane on the second monitor, then click the camera on the map. Live video from the camera is displayed in that pane. If the selected pane is already displaying live or recorded video, this is replaced with video from the map camera. If no pane is selected, video is displayed in a free pane on the second monitor. If no pane is free, video is displayed in a popup window.
- If one of the video panes on the second monitor is displaying a Video-wall, you can display video from map camera links in the second monitor. Select the pane showing the Video-wall and click a camera icon on the map. Live video from the camera is displayed on the Video-wall that is selected on the second monitor.

Clicking Upper Level opens another map:

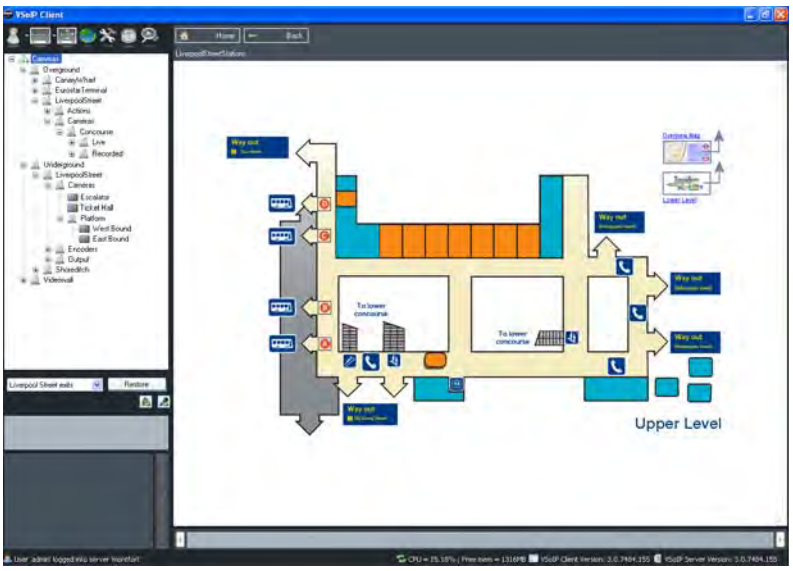


Figure 81 Liverpool Street mapset — upper level

In Figure 81, only two links have been added so far — to the overview and lower level maps. Other links can be added as required.

Chapter 12 – System Administration

This chapter contains information on the following:

- Restoring Factory Defaults
- Reusing Devices, Users and Groups
- Viewing System Information
- Default Settings

Restoring Factory Defaults

You can revert VSoIP Pro back to its factory default settings, as shown in Figure 82:

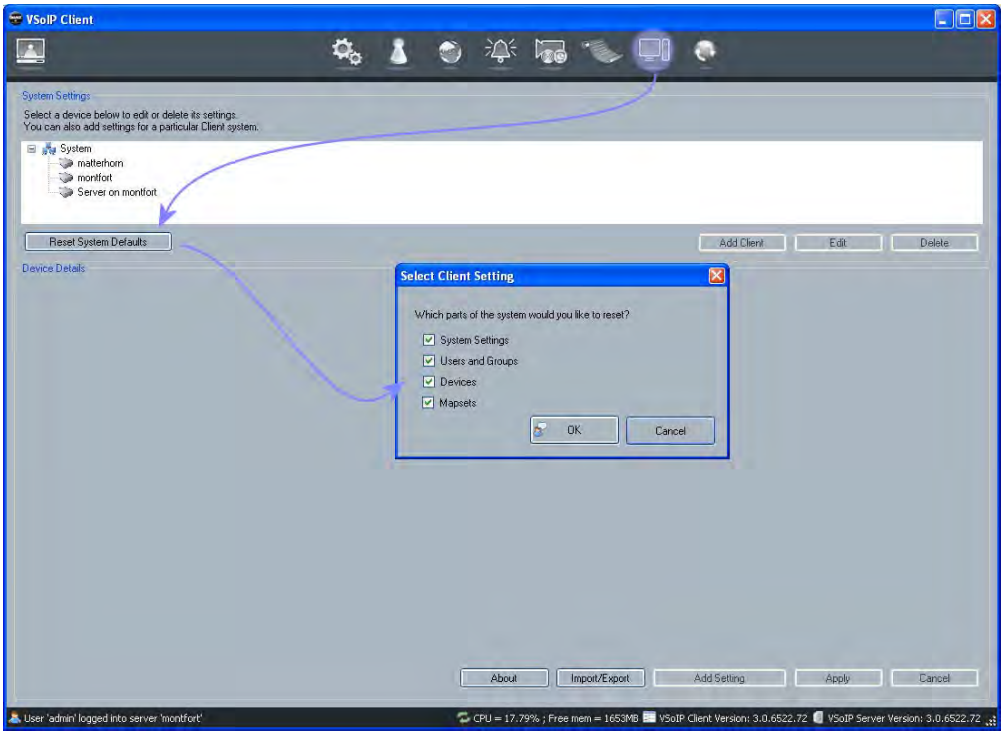


Figure 82 Restoring factory defaults

Select which parts of the system you want to reset, and click OK.

Caution: It is not possible to undo this action, so ensure that you really want to reset the settings before proceeding.

Note: After restoring to factory defaults, you must restart the client to have access to full functionality.

Reusing Devices, Users and Groups

When you have finished setting up your site and all site components (devices, users etc), we recommend that you use this process to make a backup of your site, in case of data corruption.

Caution: Note that client settings which override the defaults are not stored, nor are mapset details.

Exporting Devices, Users and Groups

Figure 83 shows how to export from VSoIP Pro.

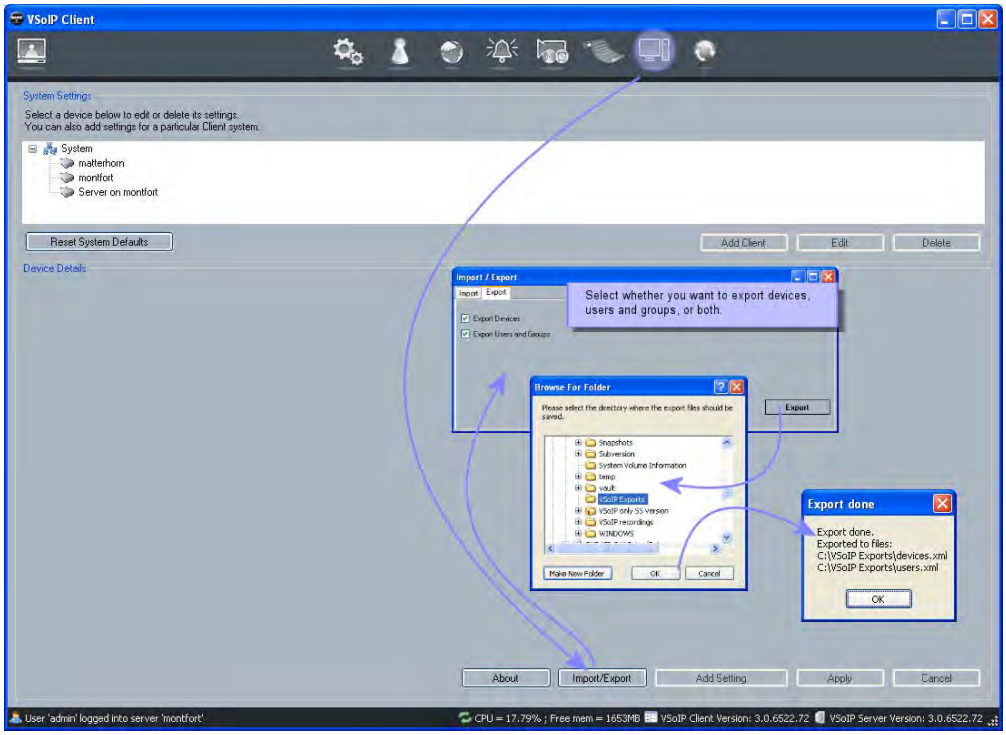


Figure 83 Exporting from VSoIP Pro

The exported data is saved in .xml format.

Importing Devices, Users and User Groups

To import device, users and user group information that you have exported, follow the instructions in Figure 84:

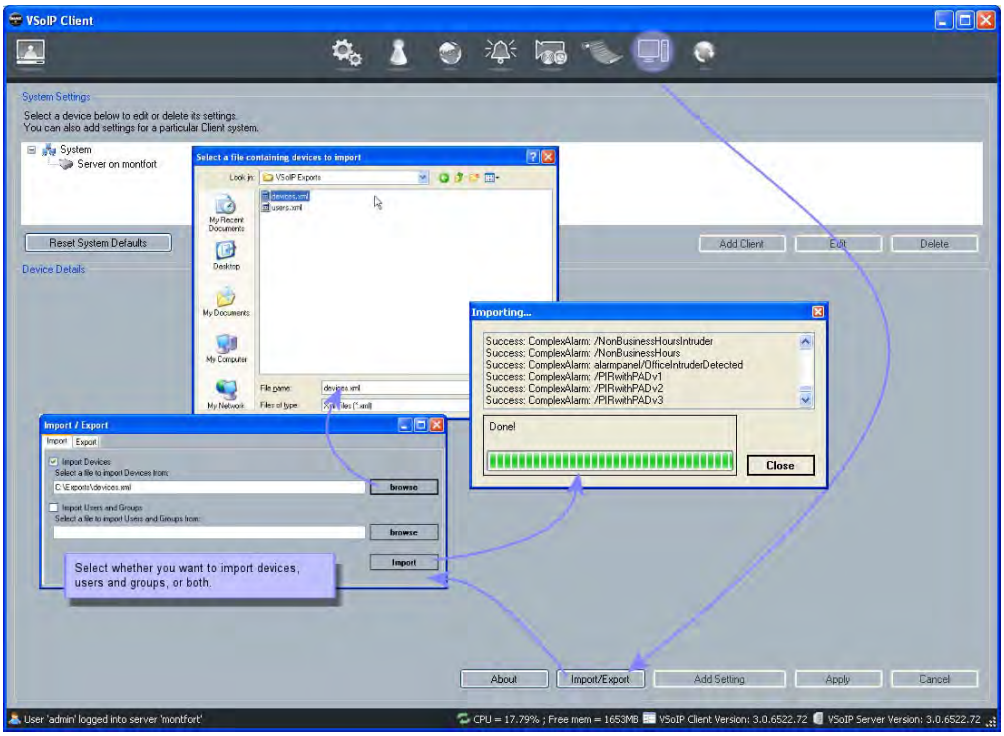


Figure 84 Importing devices into VSoIP Pro

Viewing System Information

You can view details of the current installation of VSoIP Pro, as shown in Figure 85:

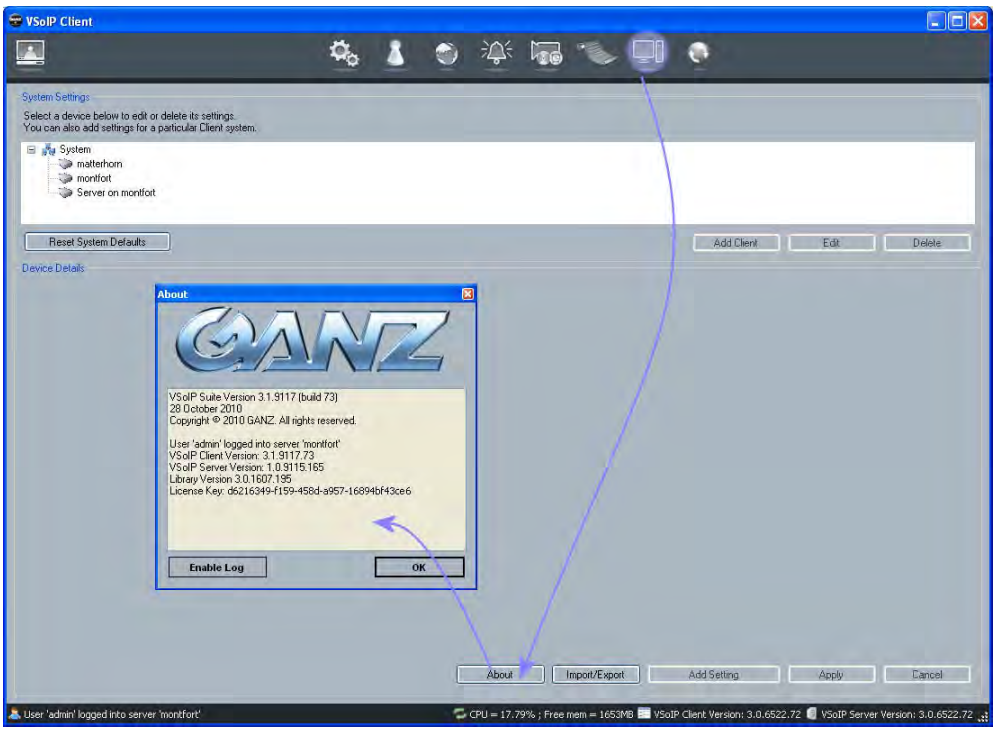


Figure 85 Viewing installation details

Default Settings

When you first view the System Settings window, the server is displayed in the device tree.

The server specifies default settings, such as inactivity timeout, aspect ratio, PTZ timeout etc. By default, these settings are used for all clients. To change a value for a particular client, see “Changing Client Settings” on page 117.

Figure 86 shows how to view these settings, and change them if required.

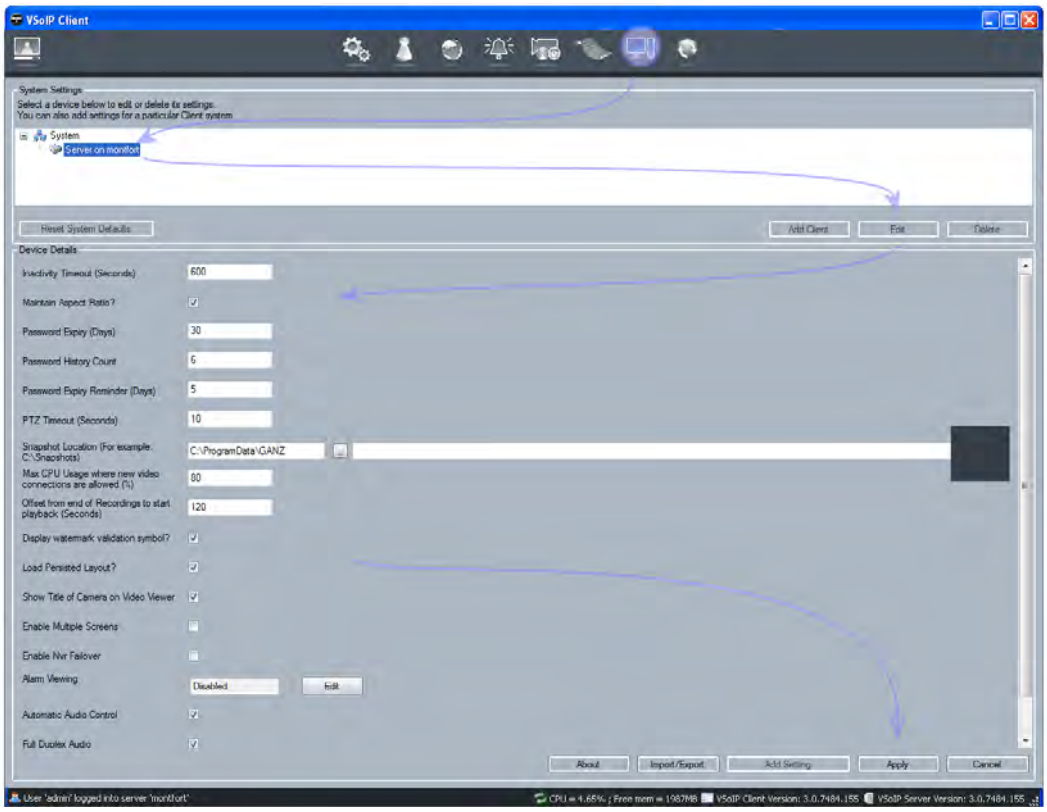


Figure 86 Viewing existing settings

Note: If you change a server default value, this change automatically applies to *all* clients connected to that server.

The following settings are available:

Table 9 Available client settings

Setting	Meaning	Default Value
Inactivity Timeout	Length of time that the client can be inactive before a password is required to access functionality again. Setting this value to zero means that the client never times out.	600 seconds
Keep Aspect Ratio	Maintain correct aspect ratio of video panes, even when they are resized.	On
Password Expiry	Length of time before a password expires and must be changed.	30 days
Password History Count	The number of different passwords that must be used before a password can be reused.	6
Password Reminder	The number of days before a password expires that you are reminded to change it.	5
PTZ Timeout	Length of time that a PTZ camera can be inactive in a video pane before the PTZ controls must be reactivated.	10 seconds
Snapshot Location	The folder where snapshots from live and recorded video are stored. VSoIP Pro automatically creates separate sub-folders for live and recorded snapshots. **Note:** This is the path on the computer running the client software component rather than a path on the computer running the server.	C:\WINDOWS\system32\config\systemprofile\Desktop

Table 9 Available client settings (Continued)

Setting	Meaning	Default Value
Max CPU Usage	The maximum CPU usage at which new video connections are allowed. This prevents overdriving the system by preventing new connections starting when the current displayed video is consuming more that this maximum value.	80%
Playback Offset Time	When playing back a recording by dragging and dropping it onto a playback pane, this is the number of seconds before the current time at which video starts playing, for example, now, minus 120 secs.	120 seconds
Show Watermark	Specify whether a red or green square is displayed on recorded video to indicate the integrity (or not) of a recording.	On
Load Persisted Layout	When opening the application, display the same cameras and layout that were in use when the application shut down.	On
Show Title of Camera in Video Viewer	Display the camera name (and path) on the top left of video panes which are displaying live video. **Note:** This setting does not apply to video displayed in the client via a Video-wall. For information on how to display overlays on a Video-wall itself, see the Video-wall User Manual.	On
Enable Multiple Screens	Allow live and recorded video to be displayed on more than one monitor.	On
Alarm Viewing	Please see “Alarm Viewing” below.	Disabled
Enable NVR Failover	Allows VSoIP Pro to reassign a recording job to another partition in the same partition group, on a different NVR, if the original NVR becomes unavailable.	Enabled
Automatic Audio Control	When interacting with a device that supports audio, this option allows a user to hear audio from a camera by playing in the active pane. For more information, see “Listening to Audio from a Camera” on page 49.	Enabled
Full Duplex Audio	Allows communications in both directions simultaneously. Disable this option to enable Half-Duplex mode.	Enabled
Audio Out Timeout	This value specifies how long a microphone can be used for before the connection times out	10 seconds

Alarm Viewing

These options determine if and where alarm video is displayed. Click Edit to specify this behaviour. The behaviour differs slightly depending on whether you have a multi-monitor setup or a single monitor.

Multi-monitor Setup

- **Disabled** — When an alarm is triggered, no video for that alarm is displayed in any pane.
- **Dynamic** — This option applies **only** to the **second** monitor.

  When enabled, VSoIP Pro automatically increases or decreases the number of video panes shown on a second monitor as needed, to display video which has been started as a result of an alarm. Note that remote client viewing must have been enabled for that alarm, (see “Displaying Live Video on all Connected Clients and Video-walls” on page 76). As alarms are manually stopped by the user, or acknowledged (either manually or automatically), the number of panes required reduces.

  Note: When the Dynamic option is selected, cameras cannot be manually dragged and dropped onto the second monitor.

- **Fixed** — This option applies **only** to the **second** monitor.

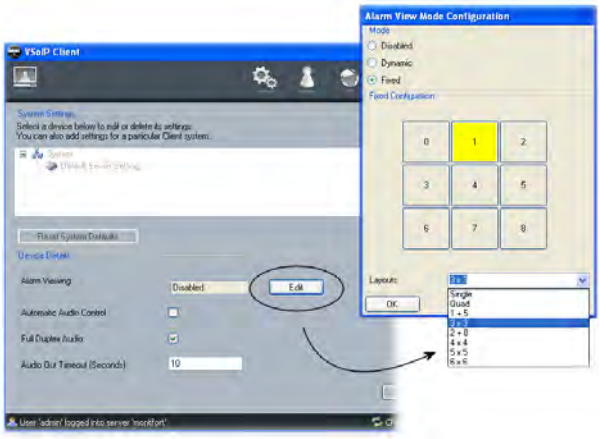


Figure 87 Specifying where alarms should be displayed

Select Fixed, and choose a pane where you want video triggered by an alarm to be displayed. Select the layout that is to be used by the second monitor. (This layout is used all the time by this monitor.) Click OK.

When an alarm (which has remote client viewing enabled) occurs, alarm video appears in the selected pane. If a subsequent alarm occurs, it is queued in the alarm stack until the first alarm is either acknowledged or the alarm video is manually stopped by the user.

Single Monitor Setup

- **Disabled** — When an alarm is triggered, no video for that alarm is displayed in any pane.
- **Dynamic** — This option is not applicable when using a single monitor, and is ignored if selected.
- **Fixed** — Select Fixed, and choose a pane where you want video triggered by an alarm to be displayed. Select the layout that is to be used when an alarm is triggered. Click OK

Note: Alarm-based video is only displayed when VSoIP Pro is viewing live video. If VSoIP Pro is not displaying live video when an alarm is triggered (for example, if the user if playing back recordings or is carrying out configuration), any alarm-based video is "queued" until the user switches to live view or the alarms are acknowledged.

Note: The server must be restarted after any Alarm Viewing changes.

Changing Client Settings

By default, all clients take their system values from the server. To change values for a particular client, you must first add the client to the list, then change its values:

1 Select the server in the devices list, and click Add Client, as shown in Figure 88.

2 Enter the client name and IP address, and click Apply.

Note: The IP address must be the same IP address as the computer running the client. You can use any name but we recommend you use the name assigned to the computer under the Windows Workgroup or Domain.

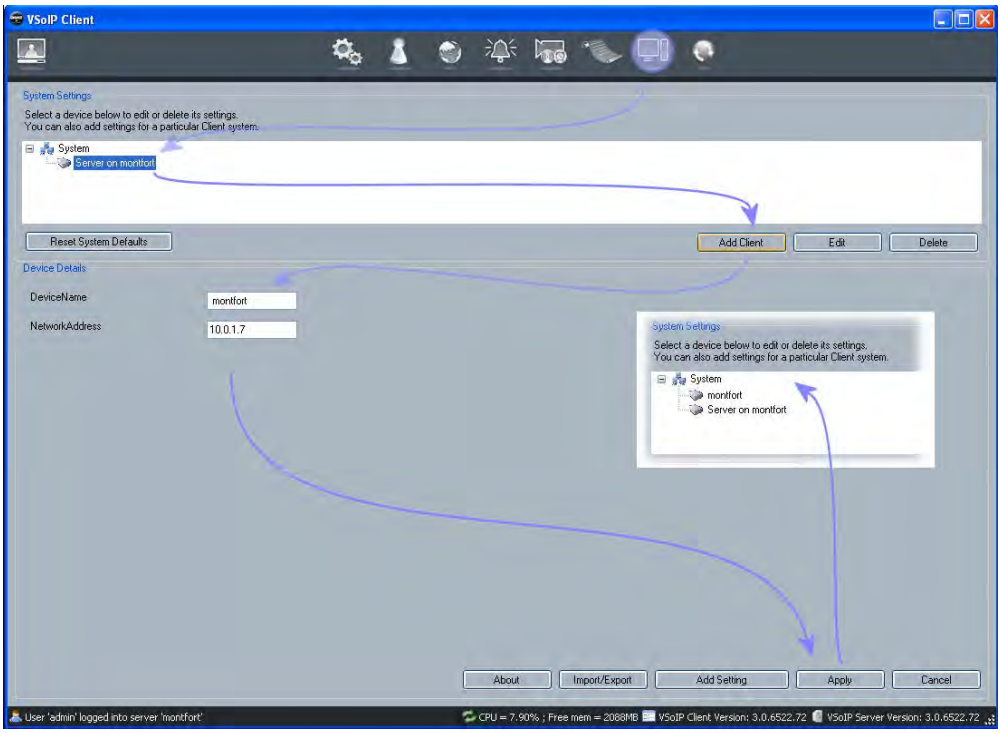


Figure 88 Adding a new client

3 The client appears in the device tree.

4 Double-click the client name in the device tree, and click Edit (Figure 89).

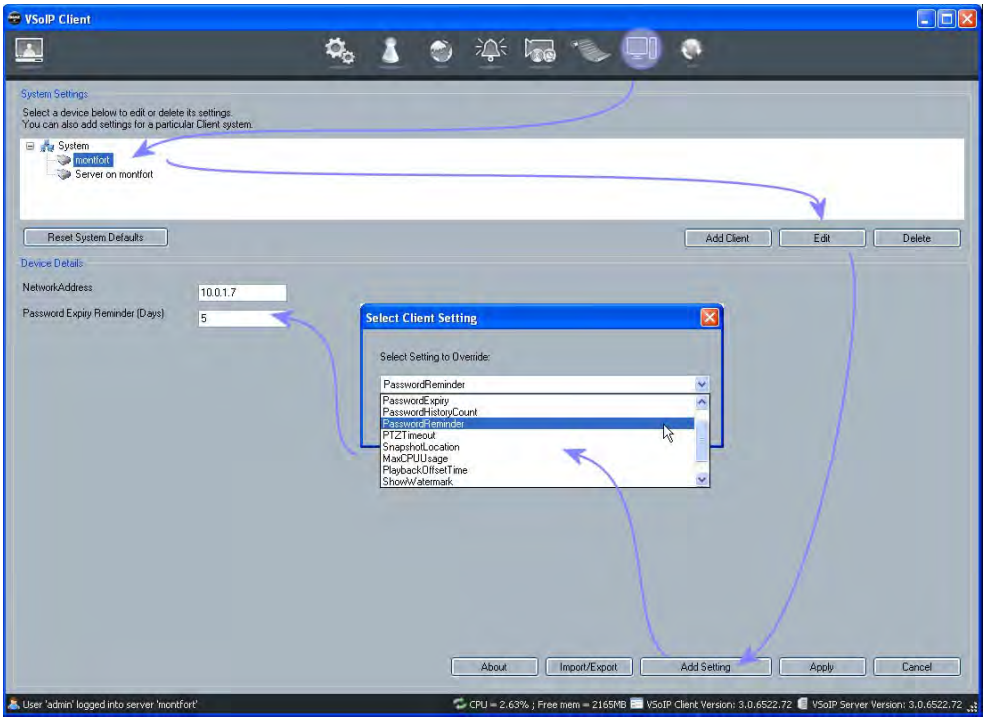


Figure 89 Overriding default client settings

5 Click Add Setting, and select the setting that you want to override from the drop-down list.

6 Click OK, and the setting appears under Device Details, with the default value shown.

7 Change this value as required, then click Apply.

8 Repeat for each setting you want to change from the default.

Chapter 13 – NVR Component

This chapter contains information on the following:

- Prerequisites
- Before Installing the NVR
- Installing the NVR
- Offline Licensing
- Upgrading the NVR
- Starting the NVR

NVR Overview

The VSoIP Networked Video Recorder software component (the “NVR”) is a Microsoft .Net framework based service for Microsoft Windows operating systems. It is designed to record media streams – primarily video feeds – from surveillance resources such as encoders, IP cameras and networked digital video recorders (DVRs).

A VSoIP NVR can run:

- As an “add-on” to the VSoIP Pro Server. The VSoIP NVR is installed by default during the VSoIP Pro Server installation process. However, to make use of its recording capabilities, you must first license the NVR.
- Independently of the VSoIP Pro Server on a different PC.

For detailed information on each installation option, see “Installing the NVR” on page 123.

The recording duties of the NVR are controlled by various “jobs” held in an SQL database. Typically the NVR works alongside a server software component (the “server”). The server allows administrative access to the NVR, communicates recording jobs, signals that various events have occurred within the surveillance system and is the authentication authority for client software (clients) requests for playback sessions, recording export, archiving and deletion.

The The NVR runs using a local system account, either LocalService or NetworkService. These accounts are built-in accounts in Microsoft Windows and do not need to be created.

Caution: When installing the VSoIP NVR on a separate PC, please be aware that the computer used to run the VSoIP NVR should not be considered to be a general purpose PC and should not be used for other tasks that might starve the NVR of system resources.

Prerequisites

Hardware

The following is the minimum hardware specification required to provide full frame rate video, without dropped frames, video corruption or latency for 100Mbps throughput (combined recording and normal speed playback).

Caution: Backing up (exporting) recordings can put significant load on the recorder particularly where backing up in non-native format is a frequent occurrence. In such cases a safety margin should be factored into the CPU power element of the PC specification to accommodate this. Since this margin varies according to the demands of transcoding the particular attributes of input format, accurate figures are only obtainable by making test back-ups on similar hardware to that proposed, measuring CPU load and scaling this up to the numbers of concurrent non-native back-ups likely to be made.

- Server or workstation, architecture 32- or 64-bit.
- Processor: 32 or 64 bit architecture CPU (e.g 32 bit Intel® Core™ 2 Quad Q6600 Quad Core Processor (or better)) 2.4Ghz.
- Memory: 4096MB.
- Hard Drive/Storage — 500GB SATA Hard Drive (or other very high performance drive).
- Optical Drive — DVDROM (for installation).
- 100 Base-T network card configured for full duplex.
- Uninterruptable Power Supply (UPS) system.

  To prevent system corruption due to power loss, a UPS system must be installed. This should be of a type that shuts down the operating system automatically if the utility power does not resume before the UPS power fails.

  To prepare for this possibility, the computer's power-on settings, operating system, and the UPS system should be configured so that the computer is powered on and the operating system is automatically rebooted as soon as utility power is restored.
- A separate drive for recordings with sufficient space to satisfy storage requirements. For information on how to calculate storage requirements, please see Appendix D, "NVR Partitions and Partition Groups".

  Storage systems for recordings should be very high speed, large capacity integrated or external Direct Attached Storage (DAS) or Storage Area Networks (SAN). On no account should Network Attached Storage (NAS) be used. Also, when configuring external DAS or SAN systems, the network delivering the video streams from the CCTV network should not be the same network used to attach the storage.

Caution: Please note that the sustained combined recording and playback bandwidth for each NVR must not exceed 100Mbps.

Operating System

The recommended operating system is Windows 7 (Pro Edition). The minimum requirement is Windows XP Professional – service pack 3, or Windows Server 2003 Standard Edition – service pack 2.

Note: The VSoIP Pro NVR has been tested and verified on Windows 7 32-bit operating systems. Installation **must** be carried out as Administrator. To run the program, you must right-click VSoIPSuite Server in the Start menu and select "Run as Administrator".

The VSoIP Pro NVR is compatible with Windows 7 64-bit operating systems.

Caution: In geographical regions where different calendar types are used, please ensure that your regional Date/Time setting is set to use the Gregorian calendar.

Additional Mandatory Software

- Microsoft .Net Framework 3.5 SP1 (includes .Net frameworks 1.1, 2,0, 3.0 and 3.5). No configuration of the .Net Framework is required.
- Windows Installer 3.1.
- Microsoft SQL Server 2005 Express Edition, Service Pack 2 must be installed followed by Service Pack 3. Any required configuration of the SQL Server should occur following the installation of the client/server, once the database for the client/server has been created.

Note: These components are automatically downloaded by the NVR installation program from Microsoft if not present at install time. They are also available from Microsoft's web-site as a download. Microsoft frequently re-designs its web-sites therefore an Internet download link is not provided. Instead we recommend that you use Google or another search engine to find the download links for the mandatory software. On examining the search results, please ensure that the download source is Microsoft.

Optional, useful software

- Microsoft SQL Server 2005 Management Studio Express — useful for changing various database settings.

Before Installing the NVR

All Operating System Settings

The PC should have the operating system installed either by the computer manufacturer or from the operating system installation media. The computer is assumed not to be the member of any Windows network domain.

Note: Changes to the operating system settings, such as changing the local or global policies relating to rights and permissions, are discouraged. These notes assume that the operating system is set up in a fresh installed state.

A single local user should be added. This should be a member of the local administrator group. NVR installation, .Net installation and SQL installation, and all maintenance should be done as this local user with local administrative rights.

Note: The NVR and SQL database engine run as Windows services and as such will execute irrespective of which user, if any, is logged in to the PC.

To prevent unscheduled system restarts, switch off the automatic Windows update feature. Updates of the Windows operating system should be carried out as part of scheduled system maintenance.

Networking Settings

- Set up the network settings for the PC and make sure that the PC network connection is enabled and connected. Check this by opening a command prompt and running the `ipconfig` Windows command-line utility, (see Appendix A, "Maintenance Information").
- Note the IP address of the NVR PC — in order for the system to make use of the NVR, its IP address must be known.
- The PC must be set up so that it can browse the Internet. During installation, the client will need to contact a licensing server located on the Internet in order to complete the installation and become licensed.
- The use of the Dynamic Host Control Protocol (DHCP) in the surveillance site is not recommended, as the VSoIP Pro Server will be unable to locate devices if their IP address are reassigned. We recommend that static IP addresses are used at all times.

Firewalls and Port Usage

For best performance, simplicity of setup and easy maintenance, it is recommended that a dedicated firewall protects the entire network rather than firewall software running on the NVR PC.

Any local software firewall should either be disabled or carefully configured so as not to prevent the NVR from contacting the licensing server. Also, any hardware firewall on the LAN should be configured to allow appropriate network access to the PC on which the NVR is executing. Some local, software-based firewalls block incoming/outgoing traffic solely on a port number basis. Others block ports to all but explicitly defined applications.

Caution: Blocking required ports and/or not allowing the NVR and related application to use the network can prevent successful installation, activation or execution of the NVR.

Table 12 details which ports are used by VSoIP NVR. These ports must be open and unused by other applications to ensure that the NVR works correctly.

Table 12 NVR port usage

Application	Role	Default Path	Port number	Description
Setup.exe	NVR installer	Installation media	80/TCP	The bootstrap installer for the NVR
.MSI file	NVR installer	Installation media	80/TCP	The main installer for the NVR
LicensingHelper.exe	NVR Licensing	C:\Program Files\GANZ\VSoIPSuite Server	80/TCP	Required to license the NVR
Services.Service.exe	NVR Application	C:\Program Files\GANZ\VSoIPSuite Server	25775/TCP	NVR Web service
Services.Service.exe	NVR Application	C:\Program Files\GANZ\VSoIPSuite Server	25776/TCP	NVR Gateway webservice

More details about port utilisation should be available in documentation supplied with the IP camera or encoder, on the manufacturer's website, or from their technical support contacts.

Additional Security Software

It is not advisable to execute the following on the NVR PC unless the impact of their execution is considered carefully:

- Anti-virus.
- Anti-spyware.
- Software firewall.

Installing the NVR

The VSoIP NVR can be used on the same PC as the VSoIP Server, or installed on a separate PC (or both). The installation procedure is similar for both, except that a different license is used.

Note: Although it is possible to run a server on the same computer as the NVR, this can lead to a conflict of resources and is therefore discouraged in all but the smallest of systems.

Using the NVR on the Same PC as the VSoIP Pro Server

To use the VSoIP NVR on the same PC as the server, you must license the NVR, as follows:

1 Ensure that the VSoIP Pro Server has already been installed on the PC.

2 Start, and then stop the server.

Note: If you forget to stop the server first, please see “NVR Installation Problems” on page 127.

3 Verify that the server’s state is marked as Stopped. For details of how to check this, see “Viewing Windows Services List” on page 148.

4 From the Start menu, select VSoIPSuite Server, and select the VSoIP Licensing Helper.

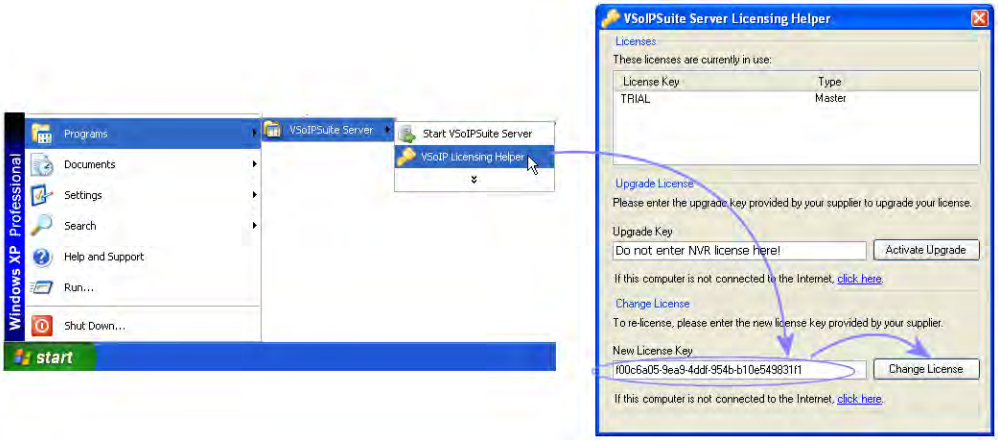


Figure 90 Licensing the NVR

5 If your computer is connected to the internet, enter the NVR License Key you have been given, as shown in Figure 90, then click Change License. Activation can take a few seconds. Licensing success, or failure, will be indicated.

Caution: Take care not to add the NVR license in the Upgrade Key box.

6 If your computer is not connected to the internet, click to license the VSoIP NVR offline, and follow the instructions in “Offline Licensing” on page 124.

Note: You must restart the VSoIP Pro Server to complete the NVR installation.

Installing the NVR on a Separate PC

To install the VSoIP NVR on a separate PC from the VSoIP Pro Server:

1 Locate the VSoIP Pro Server installation program (setup.exe).

2 Proceed through the installation until asked for a license key. Select License as stand-alone NVR and enter the NVR license key you have been given. This installs the NVR component, without the server component.

Offline Licensing

If the computer on which you are installing the VSoIP NVR is not connected to the internet, you can license it offline. The procedure is similar to that for licensing a server offline. See “Offline Licensing” on page 18 for more information.

Upgrading the NVR

You can upgrade the VSoIP NVR to increase the number of channels available for recording.

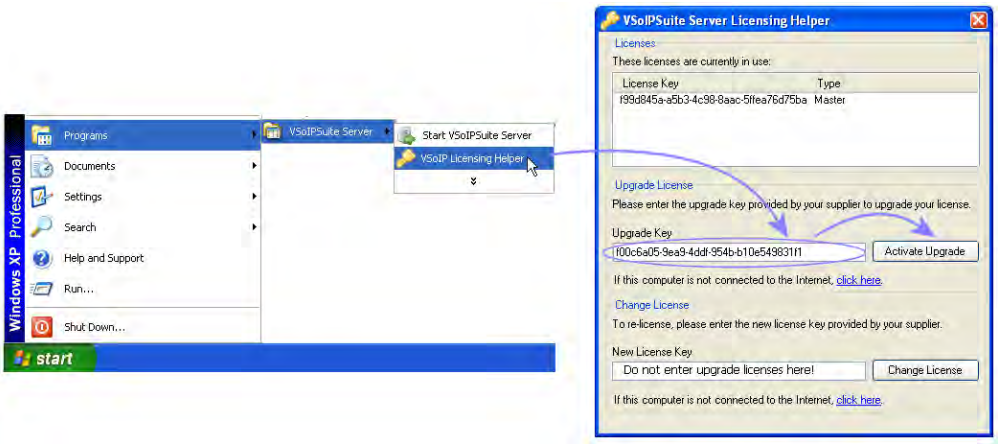


Figure 91 Upgrading the NVR

1 From the Start menu, select VSoIP NVR, and select the VSoIP NVR Licensing Helper.

2 If your computer is connected to the internet, enter the NVR Upgrade Key you have been given, then click Activate Upgrade. Activation can take a few seconds. Activation success, or failure, will be indicated.

Caution: Take care not to add the upgrade license in the New License Key box.

---

3 If your computer is not connected to the internet, click to license VSoIP NVR offline, and follow the instructions in “Offline Licensing” on page 18.

Note: You must restart the VSoIP server to complete the NVR upgrade.

Starting the NVR

Before starting the NVR, confirm the following:

- The network connection is available and configured.
- If your PC has any embedded or directly attached video capture devices, such as a USB web-cam or a video-conferencing camera, please disable these before running the NVR.

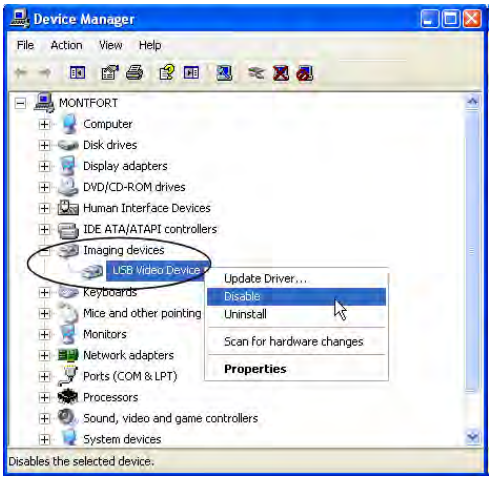


Figure 92 Disabling video capture devices

To access the Windows Device Manager, hold down the Windows function key and press the Break key. Select Hardware, the Device Manager.

The NVR runs as a Windows Service. As such it runs irrespective of whether or not a user is logged in to the computer.

Note: Using the PC for purposes in addition to running the NVR service might impact on the performance of the NVR.

The NVR can be controlled in one of two ways. Either it can be started and stopped manually, or the NVR can be started and stopped automatically when the operating system starts up and shuts down.

Starting the NVR Manually

- If the NVR is running on the same PC as the VSoIP Server, start the server. This automatically starts the NVR.
- If the NVR is running on a different PC from the VSoIP Server, select VSoIPSuite Server>Start VSoIPSuite Server from the Start menu. When restarting the computer, the NVR will not start again unless started through the Start menu.

Starting the NVR Automatically

- If your NVR is running on the same PC as your VSoIP Server, the NVR starts up when the server is started.
- If your NVR is running on a different PC from the VSoIP Server, select VSoIPSuite Server>Autostart VSoIPSuite Server from the Start menu. This signals to the NVR that it should start up and run as a background task until the computer is shut down. When restarting the computer, the NVR will be signalled to start again and to remain running as a background task whenever the computer is running.

Stopping the NVR

From the Start menu locate the server entry and choose the Stop Server option. This signals that the NVR should stop running as soon as possible. If the startup of the NVR was automatic then automatic start is switched off. The NVR will now only start when the Start menu Start Server command is chosen.

Caution: Incorrectly shutting down the recorder could risk loss of previously recorded footage, recorder system failure, or recording corruption. If this does occur and you notice that recordings are not being made or old recording not automatically deleted, then please contact your Technical Support team for additional instructions and assistance.

Disconnecting Storage Area Network (SAN) connections or external Direct Attached Storage (DAS) connections whilst the recorder is in operation could result in loss of current recordings and possible corruption of previously recorded footage.

Caution: If you do not have the necessary privileges to shut down the computer yourself then you MUST refer the matter to a user with the necessary authority to do so. DO NOT switch off the power supply to the computer as a means of shutting it down. To do so could result in irrecoverable recordings and potentially a partially or fully corrupted system, liable to fail either immediately on restarting or at some time in the future.

Troubleshooting

How can I be sure the NVR is running?

The NVR runs as part of a Windows service called Video Services (Services.Service.exe) — see Appendix A, "Maintenance Information" for more details on Windows services.

- Using the Windows services listing application, check the status of the Video Services service.
- If the Video Services service is not started then check the Windows Event Viewer application to determine what errors might be preventing startup.

Expected Performance

How many IP cameras can I record?

The NVR can record any number of IP cameras and analogue video sources attached to video encoders or Networked DVRs, up to the maximum permitted by the current license. The server component within the system contains the list of devices and allows authorised system users to set jobs to start and stop recording.

Note: The NVR does not have an enforced upper limit on the number of cameras that it can record simultaneously. Instead the system should be set up so that an NVR is not recording any more than 32 video sources simultaneously.

How many playback sessions can an NVR stream?

It is recommended that an NVR with hardware specification as given in the section “Hardware” on page 120 should have no more than 32 streams playing at one time.

Note: The system does not enforce an upper limit of playback sessions. To ensure that this limit is enforced, it is recommended that playback rights are used at the server level to restrict the number of users that can play back video within the system. A rule of thumb can be obtained from calculating the number of playback sessions likely per client (i.e. the maximum number of video panes that are likely to be switched into playback mode) and multiply this by the number of logged in users with playback rights.

What overall bandwidth can the NVR process?

There is an overall suggested maximum bandwidth of 100 Megabits per second for the host PC as described in the section “Hardware” on page 120.

Note: When considering bandwidth utilisation, remember that the proportion of the bandwidth used by a single playback session is the same (plus a slight overhead) as the stream originally recorded.

Fast-winding or rewinding recordings can use bandwidth several times higher than normal speed playback.

Recording export is an additional bandwidth consumer.

Always consider the recording, playback and export loads when deciding whether your system requires several NVRs to accommodate the recording and playback demands of your site.

Do not attempt to run the NVR beyond 60 megabits per second. Doing so might result in poor playback performance, late alarm triggered recording, and other unspecified performance issues.

NVR Installation Problems

If you are licensing the integrated NVR (on the same PC as the VSoIP Pro Server), but have forgotten to first start, then stop the server, please take the following steps:

1 Open a text editor. (Open as administrator if you are using Windows 7).

2 Navigate to C:\ProgramData\CSDataStorage.

3 Open config.xml file.

4 Change

```
<ServerIsEmbedded type="System.Boolean">True</ServerIsEmbedded>
```

to

```
<ServerIsEmbedded type="System.Boolean">False</ServerIsEmbedded>
```

5 Save file.

6 Restart the server.

Network Time Server

It is **extremely important** that all PCs running the client software and other devices use a coordinated time service.

One unified time source must be used. If this coordinated time is provided by the Windows Domain server, then ensure that the source used by the Domain is the same one used for all networked video devices.

If using a Windows Domain controller as a time source, ensure that the Windows Time service is set to automatic start-up.

Chapter 14 – NVR Configuration

This chapter contains information on the following:

- What is a Recording Job?
- Creating a Recording Job
- What Happens When a Partition Becomes Full?
- NVR Failover
- Using Stream Sampling to Reduce Required Storage Space
- Using the VSoIP NVR to Broadcast a Video Source
- Alarm-Based Recording — Pre- and Post-Alarm Buffers

What is a Recording Job?

The Networked Video Recorder records streams from IP cameras, encoders and Networked DVRs according to recording jobs created by a user.

A recording job is a set of rules which specify when footage from a video source should be recorded. A job may specify continuous recording (24/7), time-scheduled recording, or alarm-based recording. You set up recording jobs using the VSoIP Pro client application. Each recording job within the system describes:

- One video source (IP camera, encoder or Networked DVR) to be recorded.
- When the video source should be recorded, for example, by using a time schedule to specify when to record.
- When older recordings made by this job should be removed, for example, by the type of partition used, or by looping. For information on creating partitions and specifying their size, please see “Partition Overview” on page 159.

To create a recording job, you must have added at least one NVR to your surveillance site. For information on how to do this, see “Adding Devices” on page 38.

Caution: It is possible to create multiple recording jobs for the same video source, however if the times during which these jobs are recording overlap then there will be multiple concurrent recordings for that camera. If the overlap is large then this can be wasteful of recording storage space and for that reason is discouraged.

Types of Recording Job

Recording jobs may be one of the following types:

- Continuous.
- Scheduled.
- Alarm-based.

These are described below.

Continuous Recording Jobs

A continuous recording job starts to record when the job is created, and continues recording until manually stopped.

Caution: Depending on its configuration, a recording job may quickly fill up the allocated partition space: the recording job may be disabled and recording stopped. To prevent this from happening, you can:

Create the recording job on an overwrite partition — this means that the oldest recordings are overwritten once the partition is full.

Use looping to specify a time when the oldest recordings should be overwritten. See “Looping Behaviour” below. However, if you do not want recordings to be overwritten, you must ensure that the partition you are recording to is large enough to meet your needs. For information on creating partitions and specifying their size, please see “Partition Overview” on page 159.

Use NVR failover to ensure that the recording continues on another NVR. See “NVR Failover” on page 132.3

Scheduled Recording Jobs

A scheduled recording job specifies times that a recording should be made from a camera. Examples of schedules an administrator level user might create on a server are:

- All weekend — all periods for Saturday and Sunday are selected.
- Outside weekday office hours — Monday to Friday, periods representing hour long intervals after 1800h until interval prior to 0900h, are selected.
- During lunch-hour — A period of one hour after 12h00 for each weekday is selected.

Alarm-based Recording Jobs

Recording jobs can be set to start recording when an alarm is triggered. If a job is based on more than one simple alarm (a complex alarm), then recording occurs when the conditions specified in the complex alarm are met. In such situations, a single recording is made by the NVR for the length of time specified by the pre- and post-alarm values.

Note: The same complex alarm can be used to control several recording jobs. Complex alarms can be created, but disabled until required.

Complex alarms allow various different simple alarms within the system to be combined along with time schedules to provide scenarios such as:

- Record every weekend.
- Record on Monday, Tuesday and Thursday when motion is detected from a chosen number of cameras.
- Record on cameras 2, 3 and 9 when video is lost on camera 1.

See Chapter 6, "Complex Alarm Configuration" for more information regarding the creation of complex alarms. See “Alarm-Based Recording — Pre- and Post-Alarm Buffers” on page 135 for details about pre- and post- alarm recording.

Looping Behaviour

Please note the following behaviour:

- If you choose to record to an overwrite partition and do not specify a looping duration, the oldest data is automatically overwritten when the data in the partition reaches the size of the partition.
- If you choose to record to an overwrite partition and specify a looping duration, the overwrite behaviour depends on the length of the looping duration. For example, if you set a duration that would exceed the size of the partition, overwriting starts earlier than specified, once the partition is full. If you set a short looping time, for example, two hours, overwriting takes place every two hours regardless of the size of the partition.
- If you choose to record to a protected partition, any currently recording jobs are disabled as soon as the storage requirements of the recording data reach the pre-defined size of the partition. Any looping value that may have been specified is ignored.

Note: The size constraints for a partition consider *all* recordings that are being made on that partition.

What Happens When a Partition Becomes Full?

When disk space on an Overwrite partition becomes full, VSoIP Pro starts overwriting the oldest recordings on that partition.

When disk space on a Protected partition becomes 90% full, warnings are displayed. You should take action at this point to free up disk space. If disk space levels become critical, a final warning is displayed and recording stops. If you have enabled NVR failover, recording starts on another partition on a different NVR. See “NVR Failover” on page 132.

Creating a Recording Job

Caution: Recording jobs can only be created by users with appropriate privileges.

To create a recording job, you must first have added at least one NVR to the VSoIP site. NVRs are not auto-detected by VSoIP Pro and must be added manually. This applies to both integrated NVRs and NVRs installed on a different PC. For details on how to do this, please see “Adding a Device Manually” on page 40.

You must also have created at least one partition on an NVR in your site. Please see “Partition Overview” on page 159 for more information.

1 Select the camera that you want to record in the Site Explorer (Figure 93).

2 Click Create Schedule.

3 Select the required partition group from the drop-down list. If required, select the partition within that group that you would prefer to use. This preferred partition is used to store the recording job, unless it is full or the NVR is unavailable.

4 Then do one of the following:

- Select Continuous Recording to record continuously from the selected camera.
- Select Scheduled Recording, and click Show to specify the times when recording should take place.

  Note: Do not use this option to set up 24/7 recordings — use the Continuous Recording option.
- Select Start Recording on this alarm, and select the required alarm from the list.

5 Check Loop after if you are recording to an overwrite partition, and you want the NVR to automatically remove older recordings when they reach a certain age. If you want recordings to be deleted manually by a user with privileges to delete recordings, or if you are recording to a protected partition, deselect Loop after.

6 If you want to sample the recording stream for this schedule, check Sample, and select the required settings for this stream. For more information on stream sampling, please see “Using Stream Sampling to Reduce Required Storage Space” on page 133.

   Note: You can alter existing stream sampling for a schedule, for example, you can change the frames per second setting, but once enabled, you cannot disable sampling for a schedule, and vice versa.

   Note: If you select both Sample and Enable Broadcasting when creating a recording job, please note that it is the live stream which is broadcast by the NVR, and not the recorded sampled stream. If you want to create a sampled stream then you must create this using a separate Gateway Server and configure it through the web interface. Please see “Using Stream Sampling to Reduce Required Storage Space” on page 133.

7 To record audio (if available on this camera), select Enable Audio.

8 Select Enable Broadcasting to allow live video from this camera to be viewed using the same connection as the NVR. For more information, see “Using the VSoIP NVR to Broadcast a Video Source” on page 134.

9 Click Apply, then Yes.

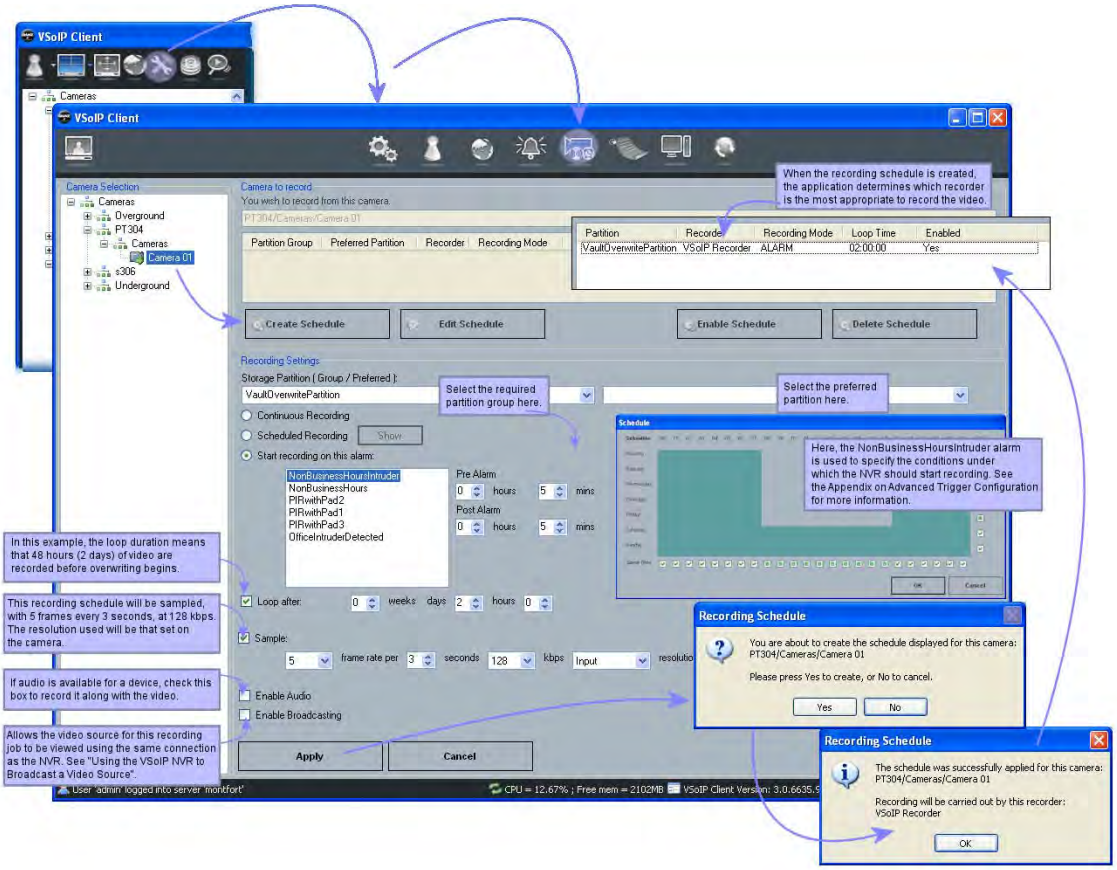

VSoIP Client
When the recording schedule is created, the application determines which recorder is the most appropriate to record the video.
Partition
Recorder
Recording Mode
Loop Time
Enabled
VaultOverwritePartition
VSoIP Recorder
ALARM
02:00:00
Yes
Create Schedule
Edit Schedule
Enable Schedule
Delete Schedule
Recording Settings
Storage Partition (Group / Preferred):
VaultOverwritePartition
Select the required partition group here.
Select the preferred partition here.
Continuous Recording
Scheduled Recording
Start recording on this alarm:
NonBusinessHoursIntruder
NonBusinessHours
PIRwithPad2
PIRwithPad1
PIRwithPad3
OfficeIntruderDetected
Pre Alarm
Post Alarm
Here, the NonBusinessHoursIntruder alarm is used to specify the conditions under which the NVR should start recording. See the Appendix on Advanced Trigger Configuration for more information.
In this example, the loop duration means that 48 hours (2 days) of video are recorded before overwriting begins.
This recording schedule will be sampled, with 5 frames every 3 seconds, at 128 kbps. The resolution used will be that set on the camera.
If audio is available for a device, check this box to record it along with the video.
Allows the video source for this recording job to be viewed using the same connection as the NVR. See "Using the VSoIP NVR to Broadcast a Video Source".
Loop after:
Sample:
Enable Audio
Enable Broadcasting
Apply
Cancel
Recording Schedule
You are about to create the schedule displayed for this camera: PT304/Cameras/Camera 01
Please press Yes to create, or No to cancel.
Yes
No
Recording Schedule
The schedule was successfully applied for this camera: PT304/Cameras/Camera 01
Recording will be carried out by this recorder: VSoIP Recorder
OK

Figure 93 Creating a recording job

Why Can’t I Create a Recording Job?

If you get an error message when setting up a recording job, please check the following:

- Ensure that you have not exceeded the number of recording jobs allowed by your NVR license.
- Check that the device you are trying to record from is online.
- Check that your SQL database has enough space to schedule the recording.

Editing Recording jobs

An existing recording job can be edited to use an alternative set of rules about when to record, e.g. a different schedule, switching on or off the looping functionality, or changing the loop duration. If the recording job for that video source is no longer required then the recording job can be deleted or disabled.

It is not possible to change the partition used for a recording job once you have created it or to have two jobs for the same video source record to the same partition — however, you can create a new recording job for the same video source, and select a different partition.

Note: If a recording job is displayed in the list of jobs, but cannot be edited, this may be because the NVR on which the job was originally set to record is no longer available, and an alternative NVR is currently being sought on which to record the job.

Note: It is not possible to change the video source of a recording job. However it is possible to have many jobs that record video from the same source, as long as they record to different partitions.

Disabling/Deleting Recording jobs

You may want to temporarily disable a recording job, for example, if the partition onto which a job is recording is becoming full, and you want to manually delete some recordings to free up space. To do this, select the required job and click Disable Schedule. To enable it again, click Enable Schedule.

Note: Disabling a job does not affect existing recordings associated with this job.

You can also permanently delete a recording job if it is no longer required. (Remember that you can edit a job to use different recording criteria, for example, time schedule or looping policy.)

To delete a recording job, select the required job from the list and click Delete Schedule. VSoIP Pro alerts you that all recordings in the partition associated with that job will be deleted too. Click OK. The recording job is no longer displayed.

Caution: Please consider the legal implications of data storage in your country/state, and the length of time for which recordings may be stored before they must be deleted.

NVR Failover

You can make use of NVR failover to ensure that a camera continues to record, even if the NVR recording it becomes unavailable.

Note: NVR failover is a system-wide setting and applies to *all* NVRs in the site. It only applies to Protect partions.

Caution: When configuring a cluster of NVRs to be used for recording, ensure that each NVR has sufficient channel licenses to record schedules assigned to it, *plus* any schedules that may be re-assigned to it during a failover.

On the System Settings page, select Enable NVR failover:

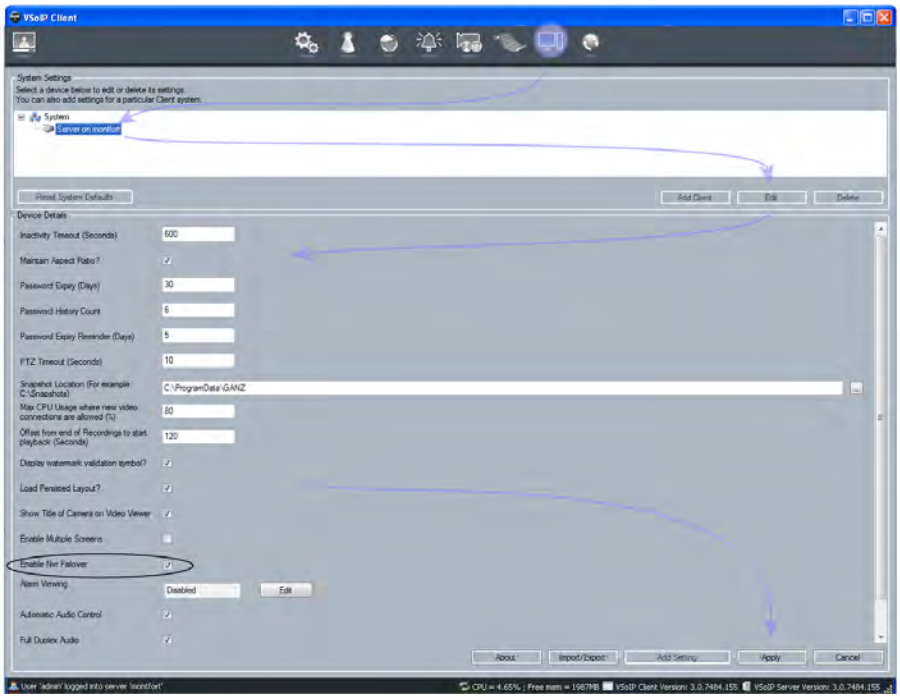


Figure 94 Enabling NVR failover

If the NVR which is recording a job fails, or its disk space becomes critical, VSoIP Pro stops recording to that NVR and automatically reassigns the job to another partition, in the *same* partition group, on a different NVR.

Note: When NVR disk space on a Protected partition becomes 90% full, warnings are displayed. You should take action at this point to free up disk space. If disk space levels become critical, recording stops on that NVR.

For more information on partitions and partition groups, see Appendix D, "NVR Partitions and Partition Groups"

Note: If the job was recording to a partition group which had only one partition in it, the recording job is not reassigned, and stops recording.

Note: If the NVR which failed comes back online, the job is not transferred back to it, but continues to record on the failover NVR.

Using Stream Sampling to Reduce Required Storage Space

You may want to record a live video stream, but need to reduce the space required to store the recording. This is known as stream sampling (or sub-sampling). For example, this allows you to reduce the recording impact of a single encoder, megapixel camera without compromising the quality of live video from the camera.

Caution: Stream sampling can greatly reduce the quality of a recording — great care must be taken to set the parameters in relation to those of the source to ensure that the resulting recording is viewable.

When creating a recording job, you can alter the input stream by choosing to record a transcoded version of it.

Note: Recordings made of transcoded streams might not be admissible as evidence in court.

- **Frames per second** — Specify how many frames per second of the input stream you want to record. Frames are **not** duplicated to achieve higher frame rates than contained in the input stream.
- **Kilobits per second** — The maximum bit rate that the transcoder can use when transcoding the input stream. A low bit rate will typically reduce image quality especially if the resolution and/or frame rate are high. There is however a limit to how low quality levels can go and this limit MAY be exceeded if the frames per second and resolution are too high.
- **Resolution** — Select the resolution required for the recorded stream. Resolution can be up and down sampled.

For all sample settings, choosing "Input" aims to keep the current characteristic of the input stream as close to that of the input stream as is possible within the constraints caused by the remaining sample settings.

The transcoder will try to achieve the requested resolution. It never duplicates frames, so the FPS setting is only achieved if the input stream's frames per second rate is equal or greater than the frames per second sampling setting. Also, the transcoder aims to stay within the specified bit rate constraints and will reduce image quality to do so.

There is a minimum image quality for sampled recording. If the chosen sampling bit-rate is too low for the characteristics of the input stream, and/or to achieve the sampling settings then the actual sampling bit-rate used will be the lowest one possible, i.e. the chosen setting will not be achieved. If you find the chosen bit-rate sampling setting is unattainable then the recordings could have higher bit-rates than you expect and there will be a reduction in the amount of recording footage that can be stored. In this case consider either increasing the storage area size or reducing the frame rate and/or resolution sampling settings to allow the transcoder to achieve the bit-rate sampling setting chosen.

Caution: Please note that the sustained combined recording and playback bandwidth for each NVR must not exceed 80 -100Mbps. When calculating the combined bandwidth, please take the following into consideration:

- The sum of the bit-rate of each recorded streams irrespective of being sampled or not-sampled

- The sum of the bit-rate of each playback non-sampled stream (each would be the same as the recorded stream bit-rate)
- The sum of the bit-rate of each playback sampled stream (each would be according to the bit-rate as a result of the sample settings)

Caution: The actual process of transcoding the stream (altering stream parameters) can be very processor-intensive, and care should be taken not to overload the CPU.

Using the VSoIP NVR to Broadcast a Video Source

VSoIP Pro allows you to view live video from the video source listed in a recording job using the same video stream as the NVR.

To do this, select Enable Broadcasting when setting up a recording job (Figure 93 on page 131).

Note: The Gateway web interface is available on the NVR, however the operation is mutually exclusive with automatic broadcasts. If Gateway broadcasts are enabled then no recording broadcasts are possible, and vice versa — if recording broadcasts are enabled then the web interface is disabled.

The resulting video stream is displayed in the tree under the NVR on which the recording job was created:

Figure 95 Video streams viewed through an NVR

Drag and drop the video streams as normal into a video pane to view live video from that camera.

Note: This broadcast stream is ONLY available for live viewing. It cannot be recorded, nor can it be used to access any other services associated with the original video source, such as PTZ etc. Furthermore, it cannot be used to access any recordings associated with the original video source.

Alarm-Based Recording — Pre- and Post-Alarm Buffers

NVR alarm-based recording causes the NVR to record when one or more triggers are fired.

Note: Unlike ordinary time-scheduled recording jobs, the server must be available for alarm-based recording jobs to function correctly.

Setting up an alarm-based recording is similar to setting up a continuous recording job but with the additional steps of specifying one or more complex alarms used to trigger recording.

To ensure that the event that causes an alarm to trigger is recorded, the recorder constantly records the video source defined in the job, for the times specified in the job (Figure 96).

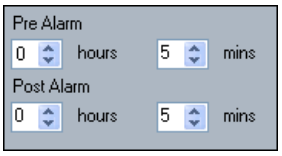


Figure 96 Pre- and post-alarm buffer settings

To manage storage overheads, the recorder makes a looped recording. In Figure 96, this value has been set to five minutes. The duration of this looped recording is known as the *pre-alarm* time. This is the duration of footage that would be preserved and made available as a pre-alarm recording if the trigger fired.

If the alarm is not triggered then older footage in the loop is discarded. However, when the associated trigger fires, the recorder automatically preserves the footage and records for a period known as the *post-alarm* time. In Figure 96, this has been set to 5 minutes. The resulting footage, pre-alarm footage and post-alarm footage are then made available as event triggered footage.

If the alarm is triggered again before the post-alarm duration of the initial triggering expires, then the elapsed part of the post-alarm is reset, causing the recorder to continue recording and resulting in an extended piece of event triggered footage.

Note: Recording footage made in this manner is not automatically deleted. The footage must be deleted by a user with appropriate privileges.

Caution: When setting up alarm-based recording jobs, you should bear in mind the number of recording channels permitted by your NVR license: the use of pre- or post-alarm buffers means that one recording channel is constantly in use, even if the associated alarm is never triggered.

Chapter 15 – Using the VSoIP Gateway

This chapter deals with the following:

- Overview
- Configuring the VSoIP Gateway Service
- Creating Sessions
- Displaying Video

Overview

VSoIP Gateway is a streaming service that services requests coming via web-pages hosted by the Stream Service itself, or from applications making use of the Service's web services interface. Video can then be viewed on any RTSP-compliant video player, such as QuickTime or VideoLan Client (VideoLan Player).

The VSoIP Gateway service can also work in conjunction with the rest of the VSoIP product range; VSoIP Pro provides viewing support in a surveillance suite, and streams from VSoIP Gateway can also be viewed on the VSoIP Video-wall.

Configuring the VSoIP Gateway Service

VSoIP Gateway is installed during VSoIP Pro Server installation and starts up when the VSoIP Pro Server starts.

To access VSoIP Gateway, enter the IP address of the VSoIP Pro Server followed by *stream*, as follows:

http://serveraddress/stream

Note: Please note that if you have enabled recording broadcasts on the NVR, then the web interface for VSoIP Gateway is disabled. For more information, please see “Using the VSoIP NVR to Broadcast a Video Source” on page 134.

The Session Config web page is displayed.

1 Click System Info on the left of the web page.

Figure 97 System Information

2 Here you can alter the default RTSP port. We recommend that you do not change the default network address or default web port as this may cause communication problems.

- Default RTSP Port — If you wish to change the default RTSP port from 554, enter the new value here. If the changed default port is in use, then the port serviced will be 7000, then 7001 etc

Caution: You must restart the VSoIP Pro Server for any changes to take effect.

Adding a Device

Once you have accessed the VSoIP Gateway service, you must add the devices you want to stream from:

1 Select Device Config on the left of the web page. The Device Config page lists the devices already created and allows you to add new devices.

2 Select a device from the drop-down list.

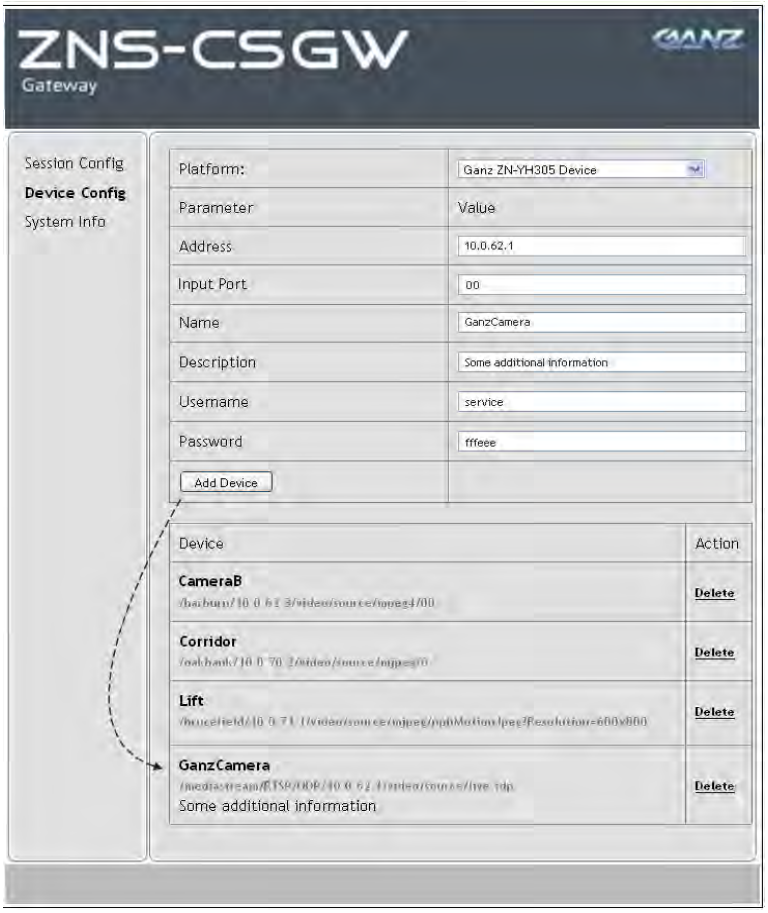


Figure 98 Adding a device to the VSoIP Gateway

3 Enter the configuration details as follows:

- **Address** — The IP address of the camera (or encoder).
- **Input Port** — Identifies which camera (on which encoder). If you only have one camera, enter 0. In Figure 98, the input of 00, which is a code for analog video input 1, encoder 1, indicates the video source.
- **Name** — The name that the device will be known as in VSoIP Gateway. In Figure 98 the device name is GanzCamera.
- **Description** — (optional) A brief useful comment about the device.
- **User Name** — (If applicable) Enter the user name used to access the device.
- **Password** — (If applicable) Enter the password associated with the user name.

4 Click Add Device. The device appears on the web page. The stream service will now request a video stream from the device. The stream received will use the settings defined when that device was configured using software provided by the device's manufacturer, or via web-pages as described in the device manufacturer's user guide.

You are now ready to create a session to view video. Sessions describe to the Stream Service how it should transcode the native stream being received from a device.

Creating Sessions

The Session Config web page lists existing sessions and allows new sessions to be created. A session describes how the stream service should transcode the stream from a previously added device. Different resolutions, frame rates, quality (Q)- values or bitrates and I-frame insertion intervals can be set. This allows the original stream from the chosen device to generate a new stream in the manner specified.

To create a new session:

1 Click Session Config on the left of the web page.

2 Enter the configuration details for this session as follows:

- **Format** — The encoded video format that you want to use.
- **Resolution** — The encoded video resolution of the output stream
- **Framerate** — The frame rate of the output stream
- **Bitrate/Quality**
  - **Bitrate** — ensures a constant bit rate (CBR)
  - **Quality** — uses a variable bit rate (VBR) to ensure constant video quality
- **I-Frame** — The number of seconds between key frames
- **Name** — The name for this session. Session names must not contain spaces.
- **Device** — The device from which video is streamed in this session

3 Click Create Session.

Note: If you have already created the maximum number of sessions allowed, the Create Session button is greyed out.

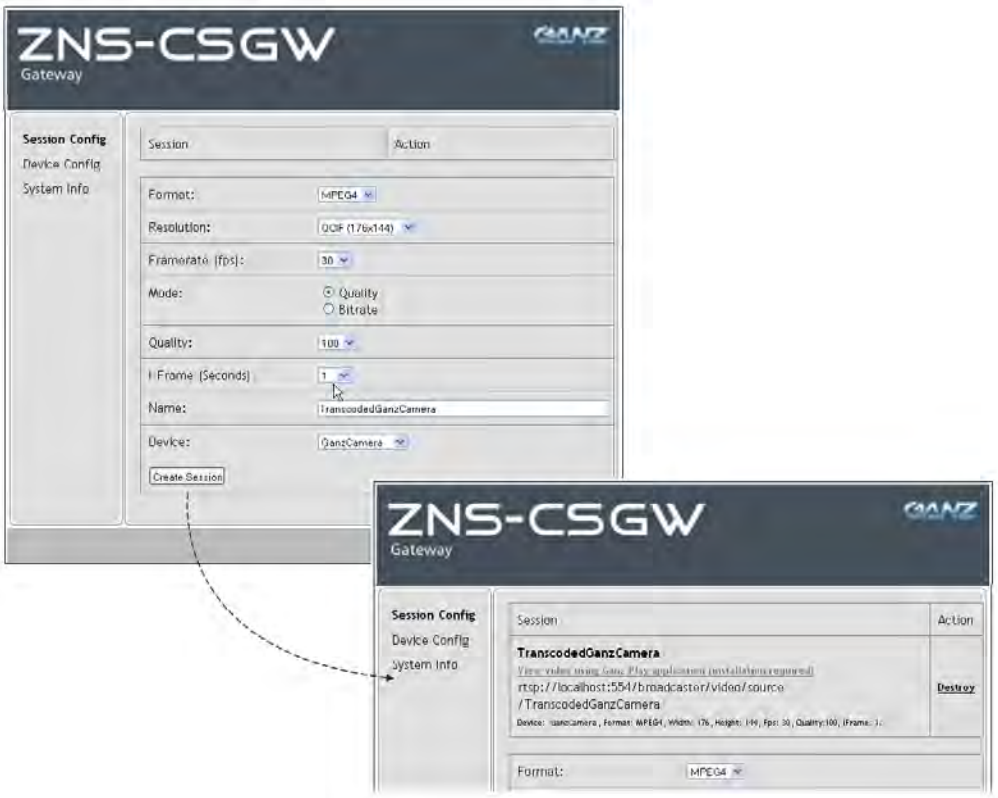


Figure 99 Creating a session

VSoIP Gateway is now actively transcoding the stream from the device, and the new session will be listed along with existing sessions.

Note: When you have created a session, you can use the System Information page to check the number of active streams and clients listed.

Displaying Video

You can display video using VSoIP Gateway:

- on web browsers running on Windows, Macintosh or Linux operating systems. Assumes that QuickTime browser plug-in or VideoLan Player browser plug-in has been installed.
- on a mobile phone using Windows Mobile Player.
- using VSoIP Player
- using VSoIP Pro running on a Windows PC, or on VSoIP Video-walls controlled by VSoIP Pro.

Displaying Video in a Web Browser

To display video in a web browser, you must have installed QuickTime or VideoLan Player.

Note: To download these, click the links on the System Config page. If you have already installed these on your PC, please ensure that the versions are at least:

- Version 7.6.8 for Quicktime
- Version 1.0.2 Goldeneye for VideoLan Player.

To display video, click the session link for the session you have created. For example, in Figure 99 this is /broadcaster/video/source/TranscodedGanzCamera.

Video is displayed in a separate pane:

Figure 100 Displaying video in a web browser

Displaying Video using the VSoIP Export Player

The VSoIP Player application is an RTSP-capable video player provided along with VSoIP Pro.

To display video from the streaming service using VSoIP Player, you must first install VSoIP Player on your PC. For information on how to do this please see the VSoIP Export Player User Guide.

1 Launch VSoIP Export Player from the Start menu.

2 When the application opens, select Open Stream from the File menu, and enter the address of the stream you want to view:

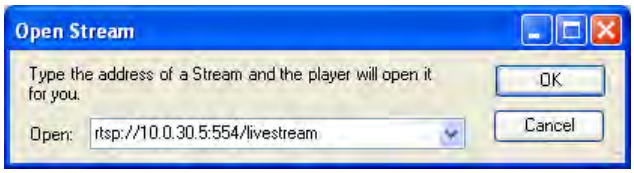


Figure 101 Opening a stream

This should be in the format:

rtsp://IPaddress:port number/*device-specific information*

(where *device-specific information* is setup and control information specific to the stream from that device)

3 Click OK to view the stream.

Displaying Video using VSoIP Pro or VSoIP Video-wall

To display video from the streaming service using VSoIP Pro, you must add VSoIP Gateway as a device to VSoIP Pro. For details on how to add a device to VSoIP Pro, please see “Adding Devices” on page 38.

Once you have added VSoIP Gateway as a device, the streams which you have created are visible in VSoIP Pro, as shown in Figure 102:

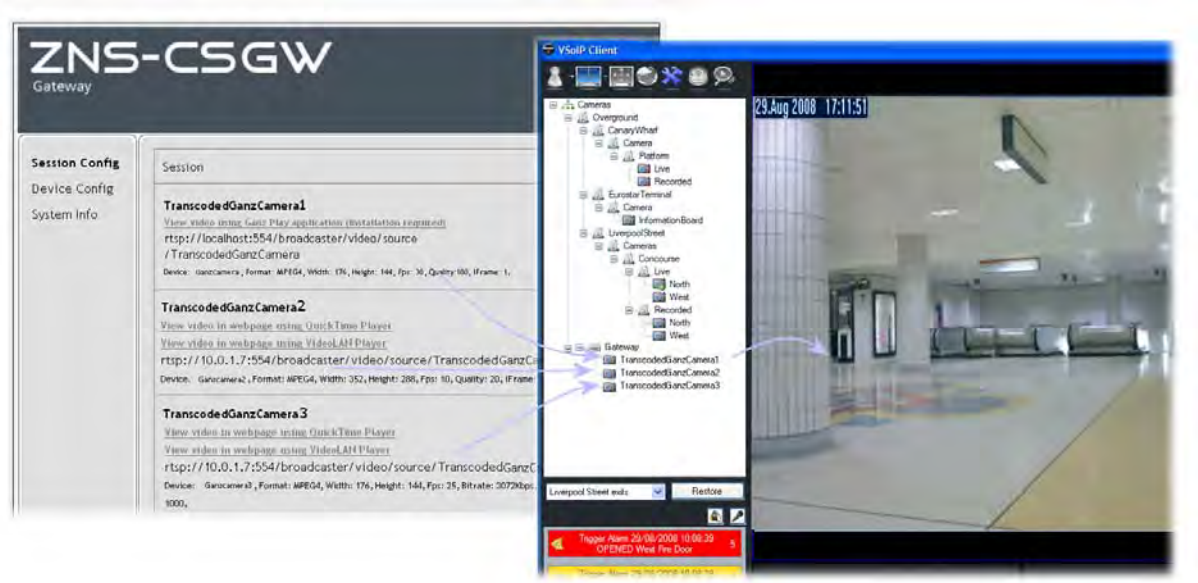


Figure 102 Displaying streams in VSoIP Pro

To display a stream, drag and drop the stream name onto a video pane.

Note: To display a stream on VSoIP Video-wall, drag and drop the stream onto a video pane on VSoIP Video-wall, as shown in Figure 103:

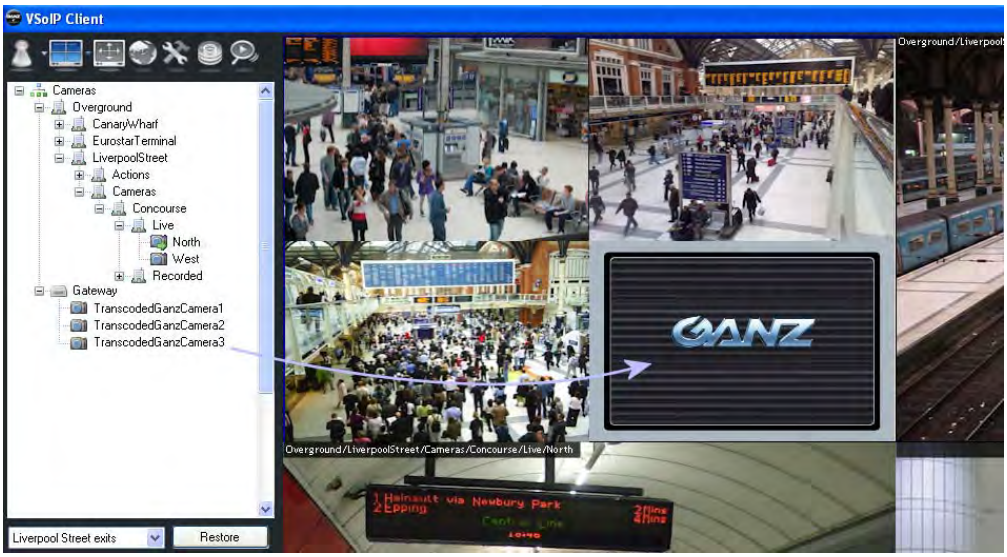


Figure 103 Viewing streams in VSoIP Video-wall

Appendix A – Maintenance Information

The follow section provides useful information regarding the general use and setup of the surveillance system.

Opening a Command Prompt in Microsoft Windows

The command prompt allows certain tools that do not have a graphical user interface to execute. Often such commands require extra parts, called arguments, that detail what options need to be configured.

For instance, the networking command `ping` allows the network connections to another networked device to be tested. The main argument required is the IP address of the device, e.g. `ping 10.11.12.13`

Note: Often the commands executed at the command prompt require certain privileges, therefore it is important to use the command prompt as an administrator level user.

Windows XP

To access the command prompt, click Start menu>All Programs>Accessories>Command Prompt. It is also often started from the Run dialog (see below) by typing **`cmd`** and clicking OK.

In the command prompt window, enter the required command at the prompt after the > character. After typing the command, press Enter to perform the command.

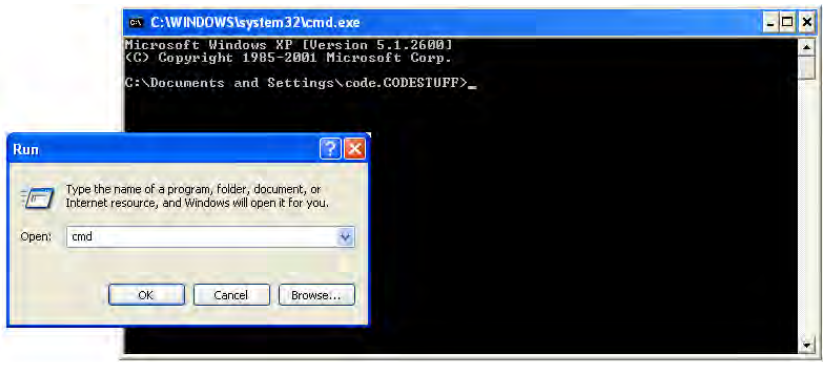


Figure 104 Opening a Windows command prompt

Opening the Run dialog

To open the run dialog, either:

- Select Start>Run, or
- Hold the Windows key and press the “R” key.

Note: If the Start menu item Start>Run is missing you can enable it by right-clicking the Start menu button. Choose Properties, select the Start Menu tab, click Customize then select the Advanced tab. In the Start menu items list-box, locate the Run command entry and check the box against it. Click OK twice to apply the change.

Finding out the IP Address of Your Computer

There are a number of ways to do this. One approach that can relied on irrespective of the Windows version being used is the command `ipconfig`.

To use `ipconfig`, open a command-prompt. Enter the command **`ipconfig`**. On entering the command, the operating system will respond with a series of addresses, note the one labelled IP Address.

Determining PC Port Usage

The Windows `netstat` command can be used to list all the network ports that are currently in use on a PC. To use `netstat`, first open a command prompt (see above), then type the `netstat` command as follows:

```
netstat -a -b
```

The command outputs a table with four columns Protocol, Local Address, Foreign Address and state. A large amount of text is generated by this command making it difficult to locate an entry. To assist in locating a particular port save the output of the command to a file using console redirection, e.g.

```
netstat -a -b > c:\portresults.txt
```

The arrow character requests that Windows not show the results on screen but instead puts the results into a file called `portresults.txt` at the root of the C drive.

Once the prompt returns, the command has complete, and the file content is ready to review. Use Windows notepad to view the contents of the results file. Use the find function in Notepad (Edit>Find) to find occurrences of number sequence, e.g. 8080. Remember that `netstat` requests the operating system to list all the ports in use so if port 8080 cannot be found by Notepad then port 8080 is free to use. If the sequence 8080 is found then that port might be in use, further analysis of the line containing the sequence 8080 is required to be certain.

If the 8080 sequence is shown under the third column - "Foreign Address" - then this line can be ignored and the search continued. Also ignore any line found that contains 8080 embedded in another number, e.g. 128080.

If line contains 8080, and the port number is not embedded in another number and the port number is under the "Local Address" column then examine the line immediately below the line to discover what application or service is using this port.

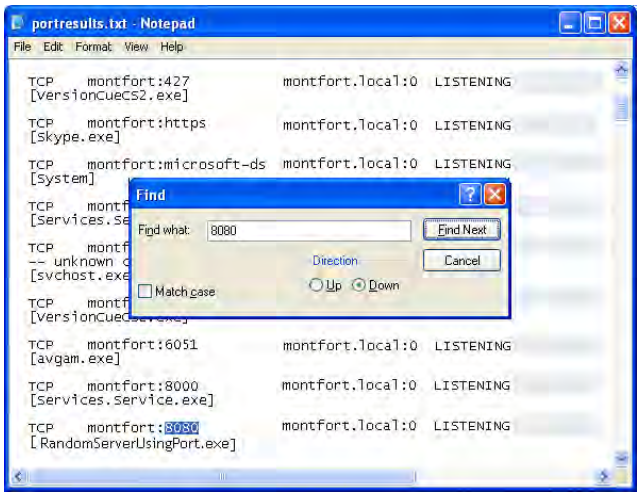


Figure 105 Determining port usage using the netstat command

The example shows viewing in Windows Notepad, the result of running the `netstat` command in a Windows Console and using console redirection to create a file containing a list of ports in use. The Find Notepad operation has been used to locate a line containing 8080, in the local address column, and the line after shows that the port is being used by an application called RandomServerUsingPort.exe.

Windows Events – Using the Event Viewer

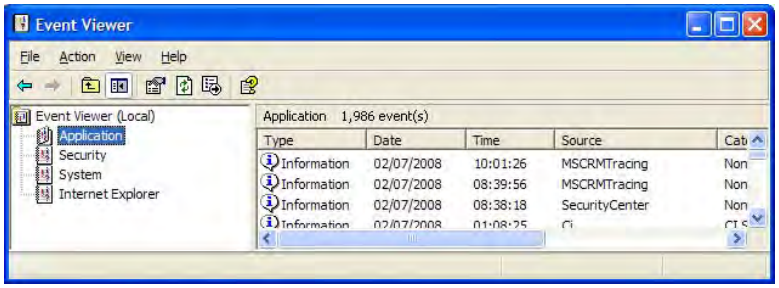


Figure 106 Windows Event Viewer

Some services and applications running on a computer need to communicate with the user but do not have a graphical interface to do so. For these services and applications the operating system provides methods of recording the occurrence of an event. All the events in the system are stored in various event logs. The Event Viewer is a convenient method of examining all events which have occurred recently. Issues concerning the proper functioning of the system are recorded and allow problems to be solved during commissioning and maintenance cycles.

Viewing Windows Logs

The Windows Event Viewer allows you to view various Windows logs. For a surveillance system, the most relevant log is the Application Log. The Application Log stores a historical list of information, warning and error messages related to applications running on the local computer.

To access this log, open the Control Panel from the Start menu and choose Administrative Tools. If the Control Panel is in category view, choose the Performance and Maintenance category, then Administrative Tools. Open the Event Viewer. Double-click the Application log.

When examining the log, note the Source column. This lists the name of the application that generated the log entry. Entries can be:

- Informational, shown with an i icon.
- Warnings, shown with an exclamation mark icon.
- Severe error, shown with a stop-sign icon.

Surveillance suite software components that have warning or error log entries should be read to determine the source of the error. The system log can be useful for finding out about computer issues that might affect the surveillance suite applications indirectly, for example low disk space.

Note: If the Control Panel entry is missing you can enable it by right-clicking the Start menu button. Choose Properties, select the Start Menu tab, click Customize then select the Advanced tab. In the Start menu items list-box locate the Control Panel entry and choose either Display as a link or Display as a menu. Click OK twice to apply the change.

Displaying Hidden or System Files

Windows XP

By default, Windows Explorer does not show hidden or system files. Because of this, you may be unable to see certain files, even though they exist on the drive.

To show hidden or system files in Windows XP:

1 Open Windows Explorer, open the Tools menu and choose Folder Options. In the Folder Options dialog, select the View tab

2 Under the Hidden files and folders section select the radio button labeled Show hidden files and folders.

3 Uncheck Hide extensions for known file types.

4 Uncheck Hide protected operating system files.

5 Click Apply and then OK.

Windows Vista

To enable the viewing of hidden and protected system files in Windows Vista please follow these steps:

1 Click Start>Control Panel menu option. When the control panel opens you can either be in Classic View or Control Panel Home view.

   If you are in the Classic View do the following:

   a. Double-click on the Folder Options icon.

   b. Click on the View tab.

   c. Go to step 2.

   If you are in the Control Panel Home view do the following:

   a. Click Appearance and Personalization.

   b. Click Show Hidden Files or Folders.

   c. Go to step 2.

2 Under the Hidden files and folders section select the radio button labeled Show hidden files and folders.

3 Uncheck Hide extensions for known file types.

4 Uncheck Hide protected operating system files. Once this is done, your Folder Options screen should look similar to the following image.

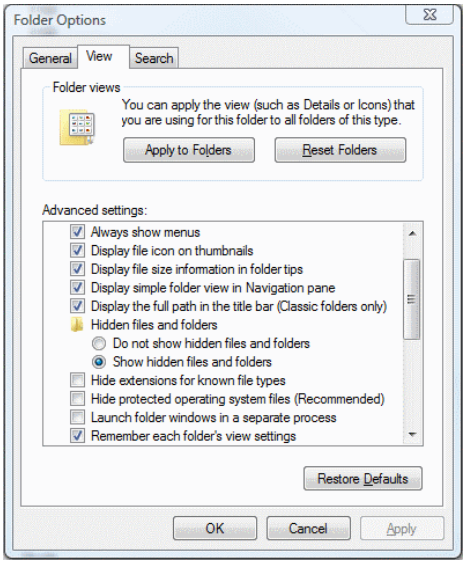

Folder Options
General
View
Search
Folder views
You can apply the view (such as Details or Icons) that you are using for this folder to all folders of this type.
Apply to Folders
Reset Folders
Advanced settings:
Always show menus
Display file icon on thumbnails
Display file size information in folder tips
Display simple folder view in Navigation pane
Display the full path in the title bar (Classic folders only)
Hidden files and folders
Do not show hidden files and folders
Show hidden files and folders
Hide extensions for known file types
Hide protected operating system files (Recommended)
Launch folder windows in a separate process
Remember each folder's view settings
Restore Defaults
OK
Cancel
Apply

Figure 107 Showing hidden files and folders

5 Click Apply and then OK.

Windows 7

If the Windows Search service is enabled on your PC, please follow these steps to enable the viewing of hidden and protected system files in Windows 7:

1 Click the Start menu button and enter "hidden" in the search programs and files box.

2 Locate and click the "Show hidden files and folders" item in the list.

3 Select Show hidden files, folders and drives (see Figure 107).

4 Click Apply and then click OK.

If the Windows Search service is disabled, please follow these steps:

1 Click Start>Control Panel menu option.

2 Select Appearance and Personalization, then under Folder Options, select Show hidden files and folders.

3 Under the Hidden files and folders section select the radio button labeled Show hidden files and folders.

4 Uncheck Hide extensions for known file types.

5 Uncheck Hide protected operating system files. Once this is done, your Folder Options screen should look similar to Figure 107.

6 Click Apply, then OK.

Configuring Application Log to Overwrite Oldest Entries

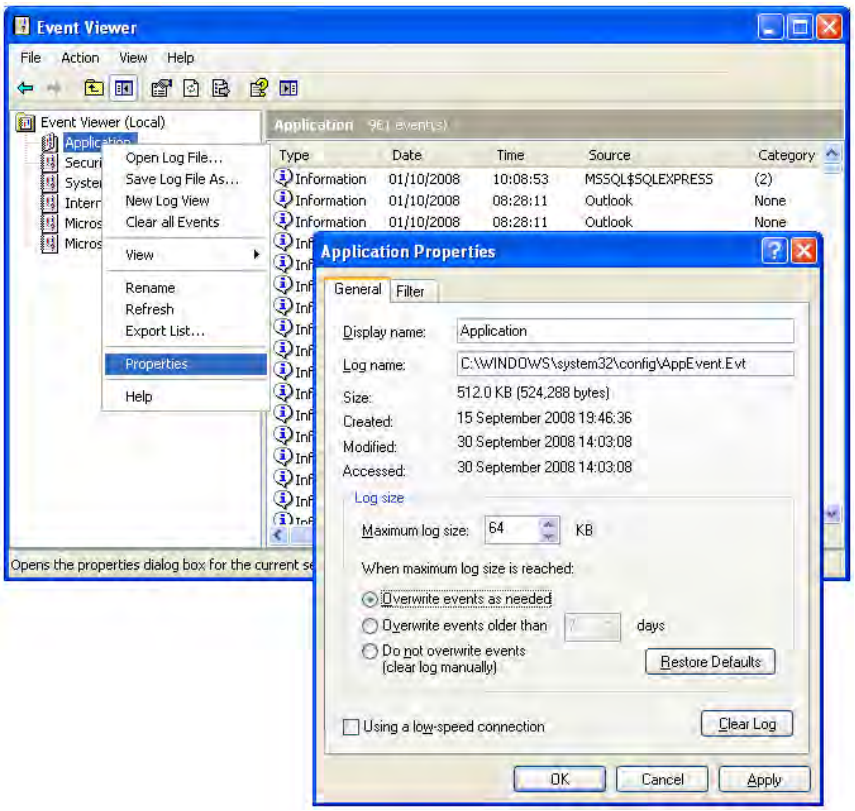


Figure 108 Changing Windows logging behaviour

The Event Log can become full and prevent proper execution of the tasks running on the computer. To prevent this, change the properties of the application event log to overwrite earliest events when there is insufficient space available.

To do this:.

1 From the Start menu open the Control Panel and choose the Administrative Tools. (If the control panel is in category view, choose the Performance and Maintenance category, then Administrative Tools.)

2 Open the Event Viewer.

3 Double-click the Application log.

4 Right-click the Application entry in the left-hand window and choose Properties.

5 In the Application Properties choose the General tab and in the Log size group click Overwrite events as needed, and click OK.

Viewing Windows Services List

Some parts of the surveillance system run as background tasks and do not require a user to be logged in for tasks to be run. These background tasks are known as services.

Although services run in the background, do not interact with users graphically, and do not require a user to be logged in, they are initiated, run and owned by a user account on the computer. Typically this account is one of the built-in accounts, usually a user called LocalService or sometimes a user called NetworkService.

Services can be automatically started or stopped by the operating system when it starts or shuts down. Alternatively, they can be manually started or stopped by a logged in user with sufficient privileges to do so.

When service-based surveillance suite components are installed, they are installed in a state that requires a logged-in user with appropriate privileges to start the service.

The Windows Services list permits a logged-in user with sufficient privileges to:

- Switch a manual service to start automatically.
- Switch an automatically starting service to manual
- Completely disable the service, preventing it from being started.

To open the Services list, from the Start menu open the Control Panel and choose the Administrative Tools option. If the Control Panel is in category view, choose the Performance and Maintenance category, then Administrative Tools. Open the Services application.

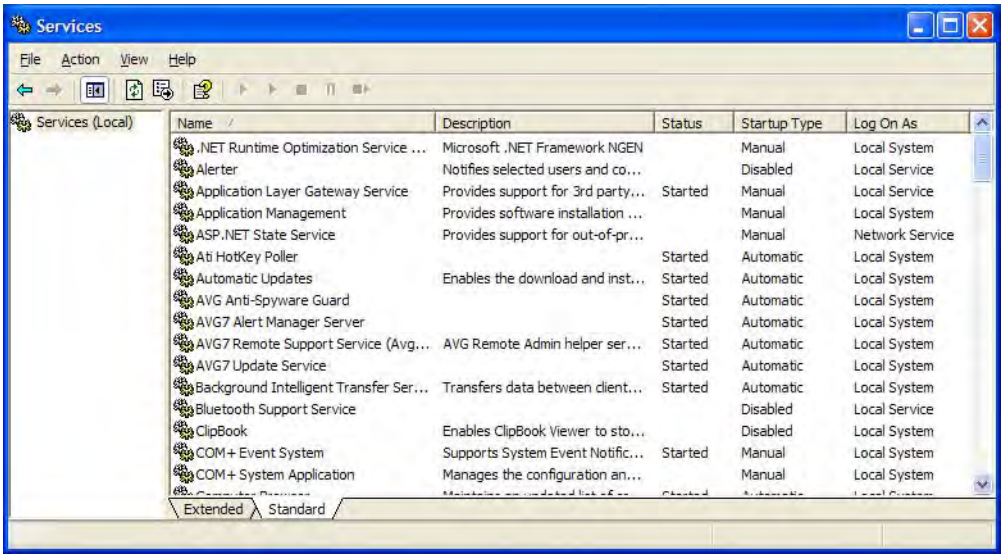

Services
File Action View Help
Services (Local)
Name Description Status Startup Type Log On As
.NET Runtime Optimization Service ... Microsoft .NET Framework NGEN Manual Local System
Alerter Notifies selected users and co... Disabled Local Service
Application Layer Gateway Service Provides support for 3rd party... Started Manual Local Service
Application Management Provides software installation ... Manual Local System
ASP.NET State Service Provides support for out-of-pr... Manual Network Service
Ati HotKey Poller Started Automatic Local System
Automatic Updates Enables the download and inst... Started Automatic Local System
AVG Anti-Spyware Guard Started Automatic Local System
AVG7 Alert Manager Server Started Automatic Local System
AVG7 Remote Support Service (Avg... AVG Remote Admin helper ser... Started Automatic Local System
AVG7 Update Service Started Automatic Local System
Background Intelligent Transfer Ser... Transfers data between client... Started Automatic Local System
Bluetooth Support Service Disabled Local Service
ClipBook Enables ClipBook Viewer to sto... Disabled Local System
COM+ Event System Supports System Event Notific... Started Manual Local System
COM+ System Application Manages the configuration an... Manual Local System
Extended Standard

Figure 109 Windows services application

Right-click and choose Properties to display the Properties dialog for the service.

Figure 110 Configuring start-up action for selected service

To request that Windows start a service when the operating system starts, change the Start-up type to Automatic. Note that the service will not actually start until Windows is re-started. To start the service from this dialog, select the required service and click Start.

To change an automatic service back to one that requires a logged-in user to start and stop the service, change the Start-up type to Manual. Note that a started service will not stop until Windows is shut down. To stop the service before then, select it in the list and click Stop.

Note: Informational messages, warnings and error events logged by services can be viewed through the Windows Event Viewer.

Checking Connectivity of a Networked Device or Computer

During installation, commissioning and when troubleshooting an installed system, it may be necessary to confirm that a particular network device is reachable. One technique is to use a network ping. This sends a special data packet over the network that the end party replies to, once received. Unless configured not to, most networked devices, IP cameras, Networked DVRs, computers running a server component, computers running a NVR component or computers running a Video-wall component will reply to incoming ping requests.

To use a network ping you need to know the IP address of the network device you wish to find.

Note: If no response is received from a pinged network device then first ensure you have the correct IP address for the device. If this is correct, then confirm that you have connectivity with other network devices before assuming that the device is not reachable. It might be that the computer from which you are issuing the ping is not able to reach some, or all networked devices due to a configuration issue with the computer you are using, a coincidental localised or wider network-connectivity issue, or the presence of a software firewall preventing ping requests being sent or received.

Sending a Ping

The following steps show how to determine whether a certain device with IP address 10.0.1.7 is available on the network. It assumes that some checks have been made to ensure that the computer being used in the test is connected to the same network as the device, and that other devices known to exist and connected to the network have responded.

1 Open a Command prompt.

2 Type **`ping 10.0.1.7`** and press Enter.

3 If the network device (or computer running a surveillance software component) cannot be reached then the response will be at least 4 lines indicating “Request timed out”.

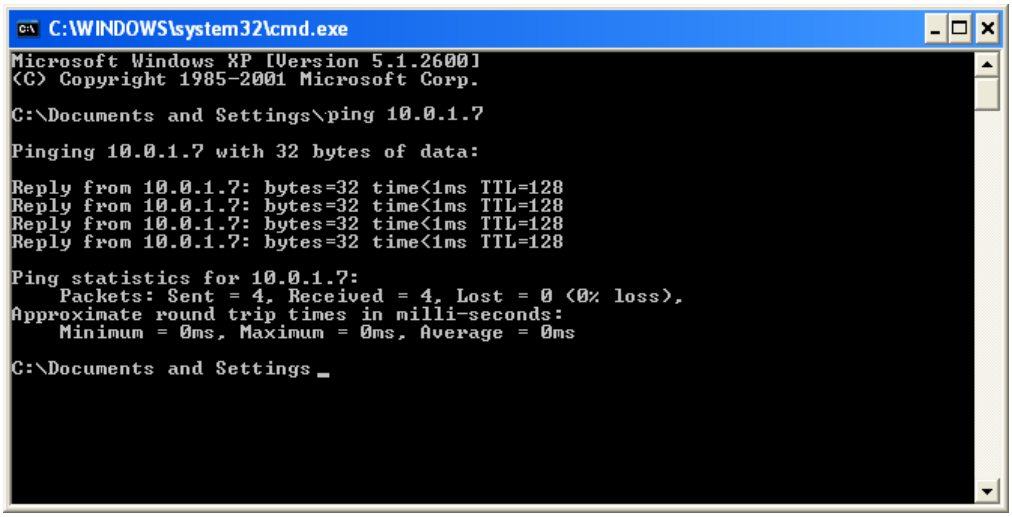

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\ping 10.0.1.7
Pinging 10.0.1.7 with 32 bytes of data:
Reply from 10.0.1.7: bytes=32 time<1ms TTL=128
Reply from 10.0.1.7: bytes=32 time<1ms TTL=128
Reply from 10.0.1.7: bytes=32 time<1ms TTL=128
Reply from 10.0.1.7: bytes=32 time<1ms TTL=128
Ping statistics for 10.0.1.7:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings

Figure 111 Successful ping reply

- If the network device was reachable then the response will contain several replies.
- If there is a mix of replies and timed out messages, this suggests that a network connection fault exists, that the network is highly congested, that the target device is too busy due to heavy workload to reply, or a mixture of these. In this case, this indicates that there is a system issue which could adversely affect the system's overall performance and could result in failed recordings, live or playback requests, and a general lack of system responsiveness.

The ping command is a useful troubleshooting tool that can highlight issues affecting the overall system and is one method that might indicate that the overall system is currently overdriven and is not operating as designed.

Troubleshooting

Troubleshooting is a complex area when the components of the surveillance suite software, the underlying operating systems, database managers, rendering engines, the different types of hardware involved and the various issues related to networking are all taken into consideration.

This section covers some typical issues that occur when installing, running and maintaining the surveillance system. It also describes how to assist a technical support representative by providing them with useful information and run-time log files to help them determine the root of a problem. It is worth noting that by examining the information provided there will be cases where the solution might be obvious and you can implement a solution without having to contact the software vendor or other support provider.

It is important to note that a high level of technical competency is required in order to perform troubleshooting. There are a number of skills required to identify the likely cause of the issues being experienced and several attempts might be required to solve problems.

It is very important to design a system from the outset rather than to make an arbitrary system using various hardware elements and using networking infrastructure that has not been optimised for surveillance use, i.e. not high bandwidth optimised. There are discussions elsewhere about the importance of design in constructing the surveillance system.

Note: It is assumed that the overall system (software, hardware and networking infrastructure) is fit for purpose and has performance safety margins that allow peaks of demand to be accommodated. It is also assumed that high performance computer hardware is used: server grade for server and Networked Video Recorder components and that all computer hardware matches or, preferably, exceeds the minimum specifications.

Caution: It is highly recommended that computer hardware is NOT used to perform non-surveillance system tasks unless the interaction between the CCTV and non-CCTV aspects of the installation can be safely accommodated within the specification of the computer and there is no shared dependency, e.g. shared database manager usage, that compromises the system.

Providing Technical Support Information

All software components have a built-in automatic log file generator. The generator is enabled whenever a special file called logging.config is detected.

Enabling Logging

To enable logging:

1 Click the System Settings icon as shown in Figure 112:

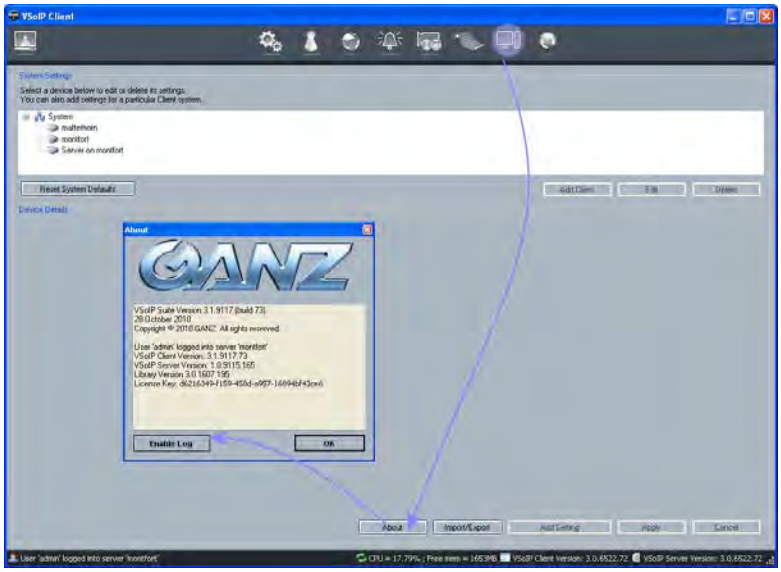


Figure 112 Enabling logging

2 Click Enable Log. This creates a file called logging.config in the installation folder.

Alternatively, you can enable logging manually, as follows:

1 Locate a suitable logging.config file and copy it into the clipboard. This will be:

- In the installation folder of the software component and called logging.config.disabled (or some other name that distinguishes it from logging.config), or
- In a sub-folder of the installation folder.

Alternatively, you might be sent the file by a technical support representative.

2 Close the application you want to log.

- For clients, exit the application.
- For servers or NVR components, stop the service controlling the application.

3 If necessary, paste the logging.config file into the installation folder. (If necessary, rename it so that it is called logging.config.)

4 Start the application to be logged.

5 Note that a log-roll.txt file will appear in one of the following locations, depending on your operating system: (the following examples are for the Client)

- Vista/Windows 7: C:\Program Data\CSLogging\VSoIPClient
- Windows XP/Server 2003: C:\Documents and Settings\All Users\CSLogging\VSoIPClient

Disabling Logging

To disable logging:

1 Click the System Settings icon.

2 Click Disable Log. The file logging.config is automatically deleted from the installation folder.

Alternatively, you can disable logging as follows:

1 Close the application currently being logged.

- For clients, exit the application.
- For servers or NVR components, stop the service controlling the application.

Note: Currently the application being logged will occasionally write to the log-roll.txt file. You will not be able to delete the log-roll file(s) or the logging.config file until the application being logged is stopped.

2 Remove the logging.config file from the installation folder by moving to a sub-folder, to another safe location, deleting it (if you have kept a copy) or renaming it to (for example) logging.config.disabled.

3 Start the application.

4 Note that after removing any log files, no more log files are added to the folder.

How Logging Works

Caution: The logging.config file contains the operating parameters for the generator and should not be modified unless you have been instructed to do so.

The log file generator automatically "rolls" the log file every hour. This means that the log-roll.txt file is renamed to a name starting with log-roll but also appends the date and hour of the day that the log started on, and a new log-roll.txt file is created containing the next hour's logging information.

This rolling behaviour has two undesirable side effects:

- When the application being logged is restarted, the log-roll.txt is deleted and a new one created. This may mean that vital error information gathered prior to the failure of the application is lost.

  To overcome this and capture the last moments of an application's behaviour in the log file, locate the log-roll.txt and rename it to, for example, log-roll-showing-UAE.txt. This means when the application being logged is restarted, the log-roll.txt will not be present to be overwritten.

  Note: If the application is still executing and you wish to capture the moment when something happens, wait until the required moment has passed, then stop the application. Once stopped, rename the log-roll.txt file as described above, and restart the application.

- If logging is enabled and the system unmaintained for an extended period, the log files may eventually consume large quantities of storage on the drive where the application is installed. This could compromise the overall performance of the computer running the application being logged.

  To overcome this, you can safely move or delete log-roll files with dates and times appended to the file's name, since these are not actively being written to by the generator. Alternatively, be sure to disable logging once your logging requirements have been met.

Caution: Logging puts extra demand on any system due to the CPU load of executing surveillance software components and log generator. This could cause system overload and result in misleading log content.

In some cases where overall system power is limited, enabling logging can put a serious load on the system, perhaps causing the system to become overdriven. Always ensure that the computer is able to accommodate the logging overhead on top of normal system operation. If this is not done, the content of the logs may be misleading since they will reveal an overdriven system rather than the fault trying to be captured. In such situations alternative approaches to troubleshooting are required.

Specifying the Logging Level

There are five logging levels:

- Debug
- Info
- Warn
- Error
- Fatal

Each logging message is assigned a level of importance, and these are reflected in these levels. For example, Debug stores **all** logging messages, whereas Fatal only stores application-critical logging messages. By default, the logging level is set to Warn.

To change the level of logging, edit the logging.config file as follows:

1 Open logging.conf in Notepad or another text editor.

2 Search for the string: <level value="WARN" />

3 Change the WARN parameter to one of the above levels, for example, <level value="FATAL" />.

4 Save the file.

Appendix B – Supported Devices

This appendix provides a list of devices currently supported by VSoIP Pro.

Devide Model	Device Type	Alarm Inputs	Alarm Outputs	Direct PTZ	TransparentPTZ	Motion Detector	NVR Recording	DVR Recording/Playback	Videowall Live Display	Encoders	Audio	Remote Config
ZN-T9000	MPEG4 Videoserver	4x	1x	N/A	YES	YES	YES	N/A	YES	2	NO	by I.E.
ZN-C9000	MPEG4 CS-mount camera	4x	1x	N/A	YES	YES	YES	N/A	YES	2	NO	by I.E.
ZN-T8000	MPEG4 Videoserver	2x	1x	N/A	YES	YES	YES	N/A	YES	2	NO	by I.E.
ZN-C8000	MPEG4 CS-mount camera	2x	1x	N/A	YES	YES	YES	N/A	YES	2	NO	by I.E.
ZN-D9000	MPEG4 dome camera	TBI	TBI	N/A	N/A	TBI	YES	N/A	YES	1	NO	by I.E.
MP1AI	M-JPEG C-mount camera	N/A	N/A	N/A	N/A	TBI	YES	N/A	YES	1	NO	by MP-Setup
MP2AI	M-JPEG C-mount camera	N/A	N/A	N/A	N/A	TBI	YES	N/A	YES	1	NO	by MP-Setup
MP3AI	M-JPEG C-mount camera	N/A	N/A	N/A	N/A	TBI	YES	N/A	YES	1	NO	by MP-Setup
MP5AI	M-JPEG C-mount camera	N/A	N/A	N/A	N/A	TBI	YES	N/A	YES	1	NO	by MP-Setup
MP1DN	M-JPEG, H264 C-mount camera	N/A	N/A	N/A	N/A	YES	YES	N/A	YES	2	NO	by MP-Setup
MP2DN	M-JPEG, H264 C-mount camera	N/A	N/A	N/A	N/A	YES	YES	N/A	YES	2	NO	by MP-Setup
MP3DN	M-JPEG, H264 C-mount camera	N/A	N/A	N/A	N/A	YES	YES	N/A	YES	2	NO	by MP-Setup
MP5DN	M-JPEG, H264 C-mount camera	N/A	N/A	N/A	N/A	YES	YES	N/A	YES	2	NO	by MP-Setup
MP8P	M-JPEG, 4CH dome camera	N/A	N/A	N/A	N/A	YES	YES	N/A	YES	4	NO	by MP-Setup
MP8D	M-JPEG, 4CH dome camera	N/A	N/A	N/A	N/A	YES	YES	N/A	YES	4	NO	by MP-Setup
ZN-PT304WL	MPEG4 PTZ indoor camera	N/A	N/A	YES	N/A	N/A	YES	N/A	YES	1	NO	by I.E.
ZN-PT304L	MPEG4 PTZ camera	N/A	N/A	YES	N/A	N/A	YES	N/A	YES	1	NO	by I.E.
ZN-D2024	MPEG4 dome camera	1x	1x	N/A	N/A	YES	YES	N/A	YES	2	NO	by I.E.
ZVS306	MPEG4 videoserve	1x	1x	YES	YES	YES	YES	N/A	YES	2	NO	by I.E.
ZN-YH305	MPEG4 CS-mount camera	1x	N/A	N/A	N/A	N/A	YES	N/A	YES	1	NO	by I.E.
DDK1500	MPEG4 dome & CS-mount camera	1x	1x	N/A	YES	YES	YES	N/A	YES	2	NO	by I.E.
C-NV4VS	MPEG4 4CH videoserver	N/A	N/A	N/A	N/A	N/A	YES	N/A	YES	4	NO	by Specific application
ZR-DHC1630NP	MPEG4 DVR	16x	N/A	YES	N/A	YES	YES	YES	YES	16	NO	by ZR-Setup
ZR-DHC830NP	MPEG4 DVR	8x	N/A	YES	N/A	YES	YES	YES	YES	8	NO	by ZR-Setup
ZR-DHC3240	MPEG4 DVR	16	16	YES	N/A	YES	YES	YES	YES	32	NO	by ZR-Setup
DR4N-DVD	MPEG4 DVR	4x	1x	YES	N/A	YES	YES	YES	YES	4	NO	by I.E.
DR8N-DVD	MPEG4 DVR	8x	8x	YES	N/A	YES	YES	YES	YES	8	NO	by I.E.
DR16N-DVD	MPEG4 DVR	16x	16x	YES	N/A	YES	YES	YES	YES	16	NO	by I.E.
DR4H-DVD	4CH H.264 DVR	4	1	YES	N/A	YES	YES	YES	YES	4	NO	by I.E.
DR8H-DVD	8CH H.264 DVR	8	8	YES	N/A	YES	YES	YES	YES	8	NO	by I.E.
DR16H-DVD	16CH H.264 DVR	16	16	YES	N/A	YES	YES	YES	YES	16	NO	by I.E.
DR4H-Lite	H.264 DVR	4	N/A	YES	N/A	N/A	YES	YES	YES	4	NO	by I.E.
DR8NRT	MPEG4 DVR	8x	8x	YES	N/A	YES	YES	YES	YES	8	NO	by I.E.
DR16NRT	MPEG4 DVR	16x	16x	YES	N/A	YES	YES	YES	YES	16	NO	by I.E.
ZN-D100VPE	H.264, MPEG4, MJPEG dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-DT350VPE	H.264, MPEG4, MJPEG dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-DNT350VPE	H.264, MPEG4, MJPEG dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.

Devide Model	Device Type	Alarm Inputs	Alarm Outputs	Direct PTZ	TransparentPTZ	Motion Detector	NVR Recording	DVR Recording/Playback	Videowall Live Display	Encoders	Audio	Remote Config
ZN-DWNT350VPE	H.264, MPEG4, MJPEG dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-D310APE	MPEG4, MJPEG dome camer	1x	1x	YES	YES	YES	YES	N/A	YES	1	YES	by I.E.
ZN-DT350APE	MPEG4, MJPEG dome camer	1x	1x	YES	YES	YES	YES	N/A	YES	1	YES	by I.E.
ZN-DNT350APE	MPEG4, MJPEG dome camer	1x	1x	YES	YES	YES	YES	N/A	YES	1	YES	by I.E.
ZN-Y11VPE	H.264, MPEG4, MJPEG CS mount camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-NH11VPE	H.264, MPEG4, MJPEG CS mount camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-NHW11VPE	H.264, MPEG4, MJPEG CS mount camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-NH21VPE	H.264, MPEG4, MJPEG CS mount camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-S100V	H.264 videoserver	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-S1000VE	H.264 videoserver	2x	2x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-S100AE	MPEG4 videoserver	1x	1x	YES	YES	YES	YES	N/A	YES	1	YES	by I.E.
ZN-S1000AE	MPEG4 videoserver	1x	1x	YES	YES	YES	YES	N/A	YES	1	YES	by I.E.
ZN-S4000AE	MPEG4 4CH videoserver	4x	4x	YES	YES	YES	YES	N/A	YES	4	YES	by I.E.
PixelPro ZN-C1	H.264 D1 CS-mount camera	1x	1x	NO	NO	YES	YES	N/A	YES	2	YES	by I.E
PixelPro ZN-C1M	H.264 720p CS-mount camera	1X	1X	NO	NO	YES	YES	N/A	YES	2	YES	by I.E.
PixelPro ZN-C2M	H.264 1080p CS-mount camera	1x	1x	NO	NO	YES	YES	N/A	YES	2	YES	by I.E
PixelPro ZN-DT1A	H.264 D1 minidome camera	1X	1X	NO	NO	YES	YES	N/A	YES	2	YES	by I.E.
PixelPro ZN-DT1MA	H.264 720p minidome camera	1x	1x	NO	NO	YES	YES	N/A	YES	2	YES	by I.E
PixelPro ZN-DT2MA	H.264 1080p minidome camera	1X	1X	NO	NO	YES	YES	N/A	YES	2	YES	by I.E.
ZN-PT-IP	H264 camera	1X	1X	YES	NO	NO	YES	N/A	YES	2	NO	by I.E.
ONVIF Generic	MPEG4/H264/MJPEG camera	N/A	0	N/A	N/A		YES			N/A	NO	by I.E.
VSoIP Gateway	VSoIP Gateway	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
VSoIP Videowall	VSoIP Video-wall v3.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
VSoIP Videowall2	VSoIP Video-wall v3.1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
VSoIP NVR	VSoIP Network Video Recorder	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Transparent PTZ protocols:	All-View Serial All-View V3 Serial BBV Serial C-Dome Serial GANZ-PT Serial	Pelco D Serial Pelco P Serial Sensormatic Serial Vicon Serial
All protocols implement:	Zoom, Pan, Tilt Presets store recall Presets renaming	OSD (when supported) Tours (when supported)

Additional Device Support

These additional devices are also supported by VSoIP Pro.

Devide Model	Device Type	Alarm Inputs	Alarm Outputs	Direct PTZ	TransparentPTZ	Motion Detector	NVR Recording	DVR Recording/Playback	Videowall Live Display	Encoders	Audio	Remote Config
ACTi 2100/2600	MPEG4 camera	2x	N/A	N/A	N/A	YES	YES	N/A	YES	1	NO	by I.E.
ACTi 4100/4200	MPEG4 camera	N/A	N/A	N/A	N/A	YES	YES	N/A	YES	1	NO	by I.E.
Axis MJPEG	MPEG4 camera	N/A	N/A	YES	N/A	N/A	YES	N/A	YES	1	NO	by I.E.
Axis MPEG4	MPEG4 camera	N/A	N/A	YES	N/A	N/A	YES	N/A	YES	1	NO	by I.E.
Arecont	MJPEG and H264 CS mount cameras	N/A	N/A	N/A	N/A	YES	YES	N/A	YES	2	NO	MP-Setup
Basler BIP-xxxx	H.264 CS-Mount	YES	YES	N/A	N/A	YES	YES	N/A	YES	2	NO	by I.E.
Basler BIP-Dxxxx	H.264 Dome	YES	YES	N/A	N/A	YES	YES	N/A	YES	2	NO	by I.E.
Basler-BIP2xxxx	H.264 CS-Mount	YES	YES	N/A	N/A	YES	YES	N/A	YES	2	NO	by I.E.
Basler BIP2-Dxxxx	H.264 Dome	YES	YES	N/A	N/A	YES	YES	N/A	YES	2	NO	by I.E.
Bosch VIPX1	MPEG4 videoserver	4x	1x	N/A	YES	YES	YES	N/A	YES	2	NO	by I.E.
Bosch VIPX2	MPEG4 2CH videoserver	4x	1x	N/A	YES	YES	YES	N/A	YES	4	NO	by I.E.
Bosch VIPX4	MPEG4 4CH videoserver	4x	1x	N/A	YES	YES	YES	N/A	YES	8	NO	by I.E.
DM NetVu	DVR	16x	N/A	N/A	N/A	YES	YES	YES	YES	16	NO	by I.E
IQeye 7xx/5xx	Camera	N/A	N/A	N/A	N/A	N/A	YES	N/A	YES	1	NO	by I.E.
Mobotix MJPEG	Camera	N/A	N/A	N/A	N/A	N/A	YES	N/A	YES	1	NO	by I.E.
Mobotix MxJPEG	Camera	N/A	N/A	N/A	N/A	N/A	YES	N/A	YES	1	NO	by I.E.
Pelco IP110	Camera	N/A	N/A	N/A	N/A	N/A	YES	N/A	YES	1	NO	by I.E.
Pelco Spectra IV-IP	Camera	N/A	N/A	YES	N/A	N/A	YES	N/A	YES	1	NO	by I.E.
UDP IPC3100	MPEG4 dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	1	YES	by I.E.
UDP IPC3500	MPEG4 dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	1	YES	by I.E.
UDP IPE1100	H.264, MPEG4 CS-mount camera	1x	1x	YES	YES	VCA	YES	N/A	YES	2	YES	by I.E.
UDP NVC1000	H.264, MPEG4 videoserver	2x	2x	YES	YES	VCA	YES	N/A	YES	2	YES	by I.E.
UDP IPE3500	H.264, MPEG4 CS-mount camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
UDP NVE 4CH series	4CH MPEG4 encoder	4x	4x	YES	YES	YES	YES	N/A	YES	4	YES	by I.E.
VSE31102	H.264, MPEG4 videoserver	2x	2x	YES	YES	VCA	YES	N/A	YES	2	YES	by I.E.
VSN36201	H.264, MPEG4 CS-mount camera	1x	1x	YES	YES	VCA	YES	N/A	YES	2	YES	by I.E.
VSN31202	MPEG4 dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	1	YES	by I.E.
VSN32202	MPEG4 dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	1	YES	by I.E.

Supported Keyboards

The following keyboards are supported by VSoIP Pro:

- VideoTec DCZ Keyboard
- WonWoo Keyboard
- GANZ ZCA-SC203 Keyboard

Please see the technical notes for the most up to date list of supported keyboards.

Appendix C – Specific Device Considerations

This chapter contains the following information:

- Adding ZV-S306 and ZN-D2024 Devices to VSoIP Pro
- Adding DRH-DVD and DR4H Lite DVRs
- Adding Generic ONVIF Devices

Adding ZV-S306 and ZN-D2024 Devices to VSoIP Pro

If you are adding a Ganz ZV-S306 or ZN-D2024 camera to the site, please note that these device types require careful configuration to ensure that VSoIP Pro receives event information from them.

These cameras have two ports, primary and secondary, which are available for connections. These ports must be configured on the camera itself.

When adding one of these devices to VSoIP Pro, you must enter the IP address followed by the primary port number, for example: 192.169.1.21:80 (where the device IP address is 192.168.1.21 and the primary port is 80).

Once the device has been added, VSoIP Pro queries it using the primary port to determine the secondary port number.

VSoIP Pro then establishes a connection to the secondary port. This allows VSoIP Pro to receive live event information, e.g. Motion Detection events.

Caution: If the secondary port number is a “well known” HTTP port for example 80 or 8080 it may be unduly affected by firewall and anti-virus software. This may prevent event information being received by VSoIP Pro.

To avoid this, please ensure that no firewall or anti-virus software is running on the same platform as the server. Alternatively, ensure that the device’s secondary port is configured to something other than a well known HTTP port.

Adding DRH-DVD and DR4H Lite DVRs

VSoIP Pro allows the following ports to be specified for these DVR types when adding/configuring the device to the site:

- RTSP_PORT: the RTSP port used for live and playback services. This port number should be appended to the IP address for the device, as follows:

  <IP_ADDRESS>:<PORT>

Caution: The default RTSP port number is 554. This number should not be changed or recording playback will not function correctly.

- ADVANCED_PORT: the port used for advanced services such as alarm notification and PTZ. This port number should be specified in the Configuration Port field.

Adding Generic ONVIF Devices

When adding a generic ONVIF device, you must append a services URL to the IP address in the Network Address field, as shown in Figure 113:

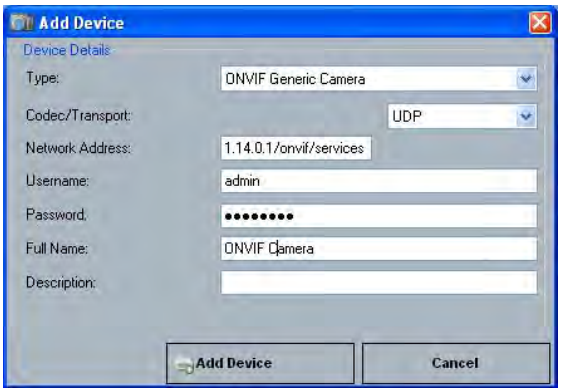


Figure 113 Adding an ONVIF device

For example, for Axis ONVIF you would enter:

`<ipaddr>/onvif/services`

For PixelPro ONVIF, enter:

`<ipaddr>/cgi-bin/onvif.fcgi`

The exact string that should be entered should be detailed in the camera documentation.

Appendix D – NVR Partitions and Partition Groups

The computing term “partition” is a widely understood one. It is used to describe a logical area of a computer storage device typically on a computer hard-drive that stores data. Within such a partition there can be many folders and files. NVR partitions are similar – they are logical areas of computer storage – but rather than being an area taken from the raw hard-drive which is then formatted to give it structure, NVR partitions are simply reserved areas of a predefined size using an existing, pre-formatted hard-drive partition.

Before you can create a recording job, you must first set up at least one partition.

Partition Overview

When creating a partition, it is important to take the following factors into consideration:

- **Size** — You should consider the data rate from the camera(s) that will be recording to that partition when deciding on the size (in Gigabytes) of a partition. By choosing a size, you are implicitly specifying the length of recording footage in minutes, hours and days, irrespective of any loop time that may have been specified.
- **Number of partitions** — There is no limit to the number of partitions you can create. We recommend that you have one partition per recorded camera. This allows the contents of a drive — i.e. which cameras have been recorded — to be readily understood at a later time should maintenance be required.

For EACH recorded camera, you should do the following:

1 Calculate the bandwidth (in kilobits per second (Kbps)) that the camera is likely to generate as a result of recording the worst case scenario. i.e. lots of motion in the encoded scene, e.g. 1536 Kbps.

2 Next, determine how many seconds of footage you wish to record from that camera, e.g. 48 hours = 48 x 60 x 60 =172800 seconds.

3 Obtain the minimum storage requirement for the camera for the required period by multiplying the bandwidth by the required duration, e.g. 1536 x 172800, or 265420800 Kb(it). Further convert to gigabytes by first dividing by 8 to obtain a kilobyte value, then by 1024 to obtain a megabyte value, and finally by 1024 again to obtain a gigabyte value, e.g.:

   265420800 / 8, or 33177600 KB.

   33177600 / 1024, or 32400 MB

   32400 / 1024, or approx 32 GB.

4 Add a 10% safety margin to the minimum storage requirement, e.g. 32 GB + 3GB, or 35GB.

5 Locate a local hard-drive that has sufficient space to satisfy the calculated storage requirement. Do not choose Network Attached Storage (NAS) or any slow speed drive such as a file server share.

6 Create a partition for the camera on the chosen drive using a meaningful name, e.g. AccessRampCameraStorage, and enter the calculated storage requirement plus the safety margin of 10%.

Remember to choose the correct partition when scheduling the recording for the camera.

Partition Modes

The NVR manages usage of each NVR partition according to the partition mode. The NVR partition modes are:

- **Overwrite** – When the content footprint in the partition reaches the size of the partition, the oldest data is automatically overwritten. Recording jobs specified as looped recordings will be forced to loop earlier than planned. Recording jobs specified as not looped will be looped. This mode keeps the most recent recordings.

- **Protected** – When the storage requirements of NVR data in the partition reach the pre-defined size of the partition, any jobs currently recording using this group are disabled and recording ends. This mode keeps the oldest recordings.

  Note: When the partition reaches 90% full, a low disk space alarm is triggered. A critical alarm is triggered when the partition reaches its pre-defined size, and recordings are disabled.

- **Archive** – This partition mode flags this position as one used to keep significant recording footage. Typically a process of maintenance has identified some recordings in an overwrite partition that need keeping, or recordings that must be deleted from a protected partition to allow the NVR to make full use of the partition. In these scenarios the recorded footage is moved into the archive partition.

Partition Groups

Partitions are organised into *partition groups*. These combine partitions from different NVRs into virtual groups. This means that you do not have to specify an exact partition when creating a recording job – the server considers which partitions belong to that group, and decides which partition is best to record to, using the following criteria:

- Available disk space on each partition
- Current recording load on each partition
- Position in the site of each NVR in relation to the camera being recorded

When creating a partition, you must specify which group it belongs to. It is strongly recommended that all partitions in a particular group are of the same type, i.e, Overwrite or Protect.

Note: If you have enabled NVR Failover (on the System Settings page, see Figure 86 on page 115), should one NVR fail, the recording job is then switched to another partition in the same partition group.

If you want to use a specific partition for a recording job, select a preferred partition from the drop-down list when creating the job (see Figure 93 on page 131).

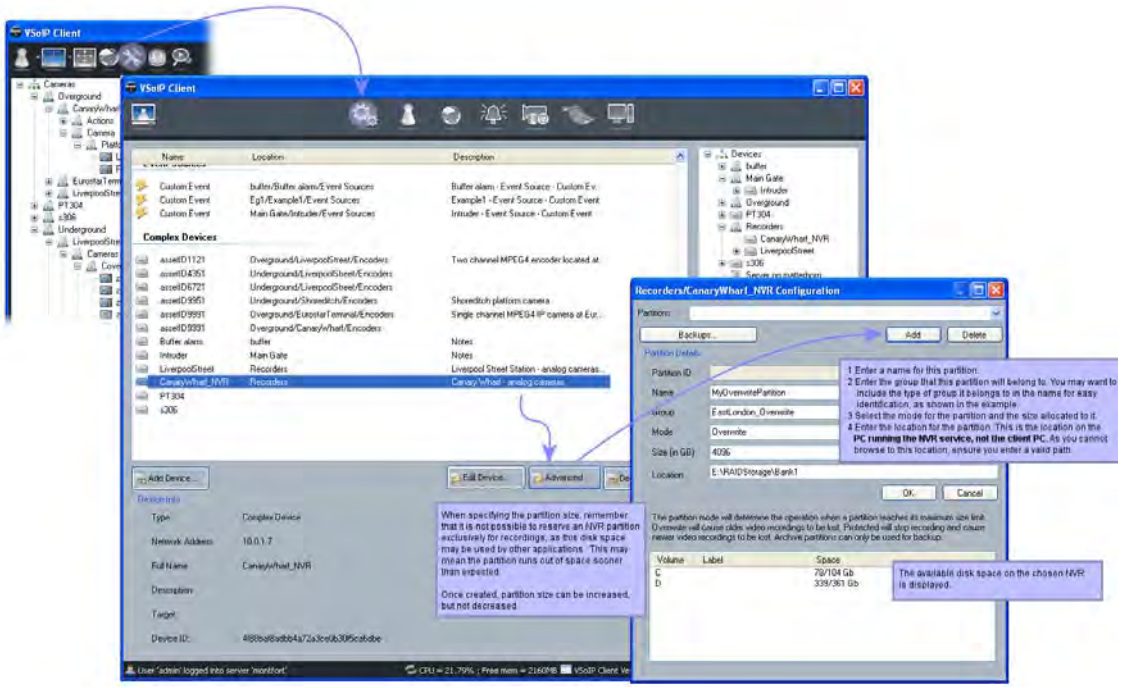

VSoIP Client
Recorders/CanaryWharf_NVR Configuration
Complex Devices
When specifying the partition size, remember that it is not possible to reserve an NVR partition exclusively for recordings, as this disk space may be used by other applications. This may mean the partition runs out of space sooner than expected.
Once created, partition size can be increased, but not decreased.
The available disk space on the chosen NVR is displayed.

Figure 114 Creating an NVR Recording Partition

When creating partitions, ensure that you do not create partitions within partitions. For example, if you specified a path E:\RaidStorage\Bank1 for one partition, and then created E:\RaidStorage\Bank1\Bank2 within it, disk space in both partitions would get used up when recordings were made to Bank2. Also, if you deleted Bank1, this would also delete Bank2.

Note: You can increase the size of a partition if required. Note that you cannot decrease the size once created.

Choosing a Recording Partition

When creating a recording job, you must specify the partition group where the recording job should be stored. The system manages the partition groups and allocates recordings to a partition within the group. NVRs within the system can contribute one or more partitions to partition groups.

Every NVR has a Default Partition Group which is selected by default when you create a recording job.

If you specify a partition group for the recording job, the system considers which NVRs contain partitions belonging to that group, and selects an appropriate NVR to record to.

In the following example, recordings from each of the four cameras are being stored on a specific partition on an NVR.

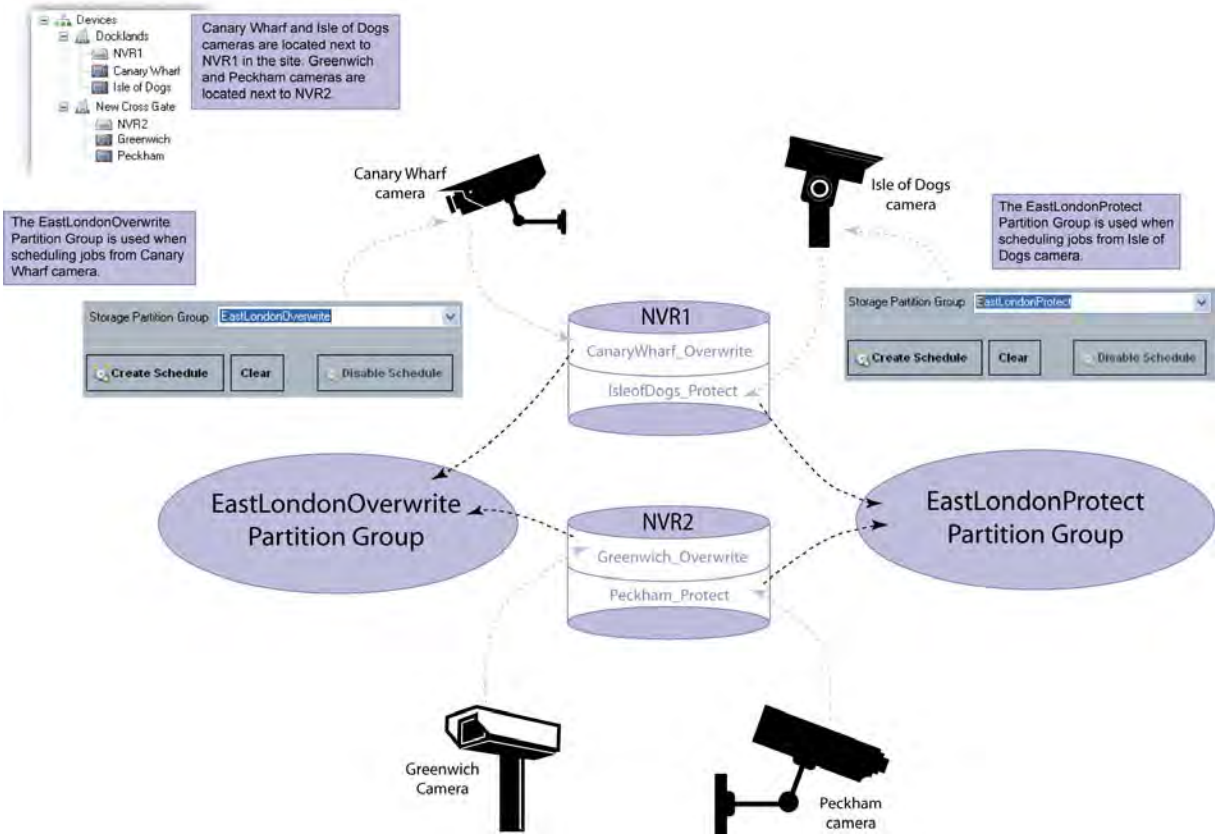


Figure 115 Partitions overview

- Footage from the Canary Wharf camera is being recorded to an Overwrite partition on NVR1, which forms part of the EastLondonOverwrite partition group.
- Footage from the Greenwich camera is being recorded to an Overwrite partition on NVR2, which is also part of the EastLondonOverwrite partition group.

When creating these recording jobs, the EastLondonOverwrite partition group was selected. The server used the above criteria to decide which partition was most appropriate for the recording job – in this case, the partition on NVR1 is logically closest to the two cameras.

- Footage from the Isle of Dogs camera is being recorded to a Protect partition on NVR1, which forms part of the EastLondonProtect partition group.

- Footage from the Peckham camera is being recorded to a Protect partition on NVR2, which is also part of the EastLondonProtect partition group.

When creating these recording jobs, the EastLondonProtect partition group was selected. The server used the above criteria to decide which partition was most appropriate for the recording job – in this case, the partition on NVR2 is logically closest to the two cameras.

Index

A

acknowledging alarms
- automatically 64
- manually 63

activating
- triggers 46

activating PTZ support 57

activation
- failure 28
- offline 18, 29
- troubleshooting 28

adding
- devices, manually 40
- devices, using autodiscovery 39
- mapsets 107
- trusted sites 26
- user groups 36
- users 32

administrators, several 31

alarm-based recording jobs 128, 129, 135

alarms
- auto-acknowledgement 64
- closing 64
- configuring 62
- copying 84
- disabling 84
- display 62
- manual acknowledgement 63
- viewing on remote clients 116
- viewing properties 63

aspect ratio, default setting 115

assigning keyboard IDs 93

audio
- listening to 49
- timeout 50

audit trail 72
- profiles 73

autodiscovery 39

B

backing up site data 112

C

camera sequences
- configuring 50
- deleting 51
- editing 51

cameras
- compatibility 8
- displaying title 116
- ZV-S306 40

changing
- client default settings 117
- device names 45
- recording jobs 131
- sequences 51

checking connectivity 149

client
- configuration 30
- default settings 115
- firewall 25
- getting started 30
- installation 28
- operating system 24
- port usage 25
- pre-installation 24
- prerequisites 23

client overview 22

closing alarms 64

command prompt, opening 143

compatibility
- cameras 8
- DVR 8

complex alarms
- auto-acknowledgement 64
- configuring 75
- copying 84
- disabling 84
- relays 78
- viewing on remote clients 116

computer's IP address, determining 143

configuring 72
- alarms 62
- audit trail 72
- client 30
- complex alarms 75
- devices 38
- devices using web interface 43
- mapsets 98
- NVR 128
- PTZ 47
- recording jobs 128
- sequences 50
- stream settings 9
- triggers 46
- user groups 36
- users 31
- video sources 45

continuous recording jobs 128

controlling PTZ cameras 57

controls, live view 53

copying
- alarms 84
- user groups 37

CPU usage, maximum 116

creating
- complex alarms 75
- mapsets 98
- new user 32
- recording jobs 128, 130
- recording partitions 161
- sequences 50
- user groups 36
- users 31

D

data loss, preventing 14

default
- password 29
- playback offset time 116
- settings, client 115
- user name 29

defaults
- administrative user 36

deleting
- devices 44
- mapsets 108
- recording jobs 132
- sequences 51
- stored views 61
- user groups 37
- users 35

determining port number 88

device information
- exporting 112
- importing 113

devices
- adding manually 40
- adding using autodiscovery 39
- autodiscovery 39
- changing names 45
- configuration 38
- deleting 44
- grouping 41
- identifying 96
- specifying location 41
- using web interface for configuration 43

DHCP, use of 16, 25, 121

Direct-X 27

disabling
- alarms 84
- logging 152
- power saving 17
- recording jobs 132
- users 34

disabling TCP/IPv6 38

displaying
- camera title 116
- recordings 65

duplicating user groups 37

DVR compatibility 8

E

editing
- recording jobs 131
- sequences 51

enabling
- logging 151

expected performance, NVR 126

exported recordings 71

exporting
- device and user information 112
- recordings 71

exporting recordings 70

F

factory defaults, restoring 111

failover 132

feedback
- preventing 50

firewalls 122
- and web device configuration 43
- client 25
- server 16

G

getting started 30

graphic sub-system 27

grouping devices 41

H
hardware driver, PTZ keyboards 91

I
identifying devices, with keyboard 96
IE8, adding trusted sites 26
importing device and user information 113
inactivity timeout, default setting 115
installing
  client 28
  NVR 123
  Player application 71
  server 17
IP addresses
  DHCP 16, 25, 121
IP addresses, determining 143

K
keyboard identifiers
  assigning 93
keyboards, PTZ 96

L
layouts
  specifying 54
  storing 60
licensing 11
  types 28
listening to audio 49
listing recordings 67
live video
  controls 53
  snapshots 56
  starting 55
  stopping 55
location text 41
logging
  disabling 152
  enabling 151
looping recording jobs 129, 130

M
main menu 53
manual alarm acknowledgement 63
manual device addition 40
map-links, associating with devices 108
mapsets
  adding 107
  configuring 98
  deleting 108
  examples 109
  overview 107
maximum number of views 52, 65
more than one administrator 31
moving from trial to full version 28
moving PTZ cameras 57
multi-monitor support 53, 54, 116
multi-users 31

N
network time server 29
NVR
  configuring 128
  expected performance 126
  installing 123
  operating system 120
  partition groups 160
  partitions 159
  port usage 122
  pre-installation 121
  prerequisites 120
  sampling 130
  starting 124
  stopping 124
  troubleshooting 126
NVR failover 132

O
offline activation 18, 29
ONVIF devices 40
opening
  command prompt 143
  run dialog 143
operating system
  client 24
  NVR 120
  server 14
overview
  client 22
  mapsets 107
  server 13
  system 7

P
pane layout 54
Pan-Tilt-Zoom
  configuration 47
partition groups, NVR 160
partitions
  creating 161
  on NVR 159
  preferred 130
  selecting 161
password
  changing 33
  default 29
  expiry, default 115
  history count, default 115
  reminder, default 115
persisted layout, loading 116
ping command, using 150
playback offset time default 116
Player application
  installation 71
Player application, installation 71
playing back recordings 67
port number, determining 88
port numbers, specifying 40
port usage
  client 25
  NVR 122
  server 16
power loss, preventing data loss 14
power saving, disabling 17
preferred partitions 130
pre-installation 121
  client 24
  NVR 121
  server 15
prerequisites 120
  client 23
  NVR 120
  PTZ keyboards 91
  server 14
preventing feedback 50
previous layout, displaying 116
profiles, audit trail 73
PTZ cameras
  control 57
  moving and zooming 57
  timeout, default 115
PTZ configuration 47
PTZ keyboards 91
  hardware driver 91
  identifying devices 96
  prerequisites 91
  software driver 91
  troubleshooting 97
PTZ support, activating 57

Q
quick login 35

R
recording footage
  synchronising 70
recording jobs
  alarm-based 129
  continuous 128
  creating 128, 130
  deleting/disabling 132
  editing 131
  looping 129
  time-scheduled 129
  types of 128
recording partitions 159
recording service, closing 125
recordings
  alarm-based 128, 135
  displaying 65
  exporting 70, 71
  listing 67
  playing back 67
  storage issues 132
  taking snapshot 69
  time-scheduled 128
recovering, stored views 61
reducing required storage space 133
relays, complex alarms 78
remote access, using web browser 88
remote clients, viewing alarms on 116
required ports
  client 25
  server 16
restoring factory defaults 111
reusing devices, users and groups 112, 113
run dialog, opening 143

S
sampling, streams 130, 133
scheduled recording jobs 129
sequences 59
  configuring 50
  deleting 51
  editing 51
server
  firewall information 16

installation 17
operating system 14
overview 13
port usage 16
pre-installation 15
prerequisites 14
starting 19
several administrators, caveats 31
shutting down recording service 125
site backup 112
snapshots
default location 115
live video 56
recorded video 69
software driver, PTZ keyboards 91
specifying
location 41
pane layout 54
port numbers 40
starting up
client 29
live video 55
NVR 124
server 19
stopping
client 29
live video 55
NVR 124
server 20
storage space, reducing 133
stored views 60
deleting 61
recovering 61
storing recordings 132
stream sampling 130, 133
stream settings, configuring 9
sub sampling 133
supported devices 154
synchronising recording footage 70
system
components 7
information, viewing 114
licensing 11
overview 7

T

taking snapshots
live video 56
recorded video 69
TCP/IPv6, disabling 38
timeout, audio 50
time-scheduled recordings 128
trial version, upgrading 28
triggers, configuring 46
troubleshooting
activation 28
NVR 126
PTZ keyboards 97
web configuration access 43
trusted sites, adding 26
types of license 28

U

Uninterruptable Power Supply 14
UPS 14
user groups
adding 36
backing up 36
configuring 36
copying 37
deleting 37
user information
exporting 112
importing 113
user name default 29
users
adding 32
changing passwords 33
configuration 31
creating new 32
deleting 35
disabling 34
logging in quickly 35
using
PTZ keyboards 91
using sequences 59

V

video
viewing remotely 88
video pane layout 54
video sources, configuring 45
viewing
alarm properties 63
alarms on remote clients 116
client defaults 115
system information 114
views, maximum number 52, 65

W

watermark, default 116
web browser, remote access 88
web device configuration, troubleshooting 43
Windows Events Viewer 145
Windows Services 148

Z

zooming PTZ 57
ZV-S306 cameras 40

Manual produced on 17 May 2011